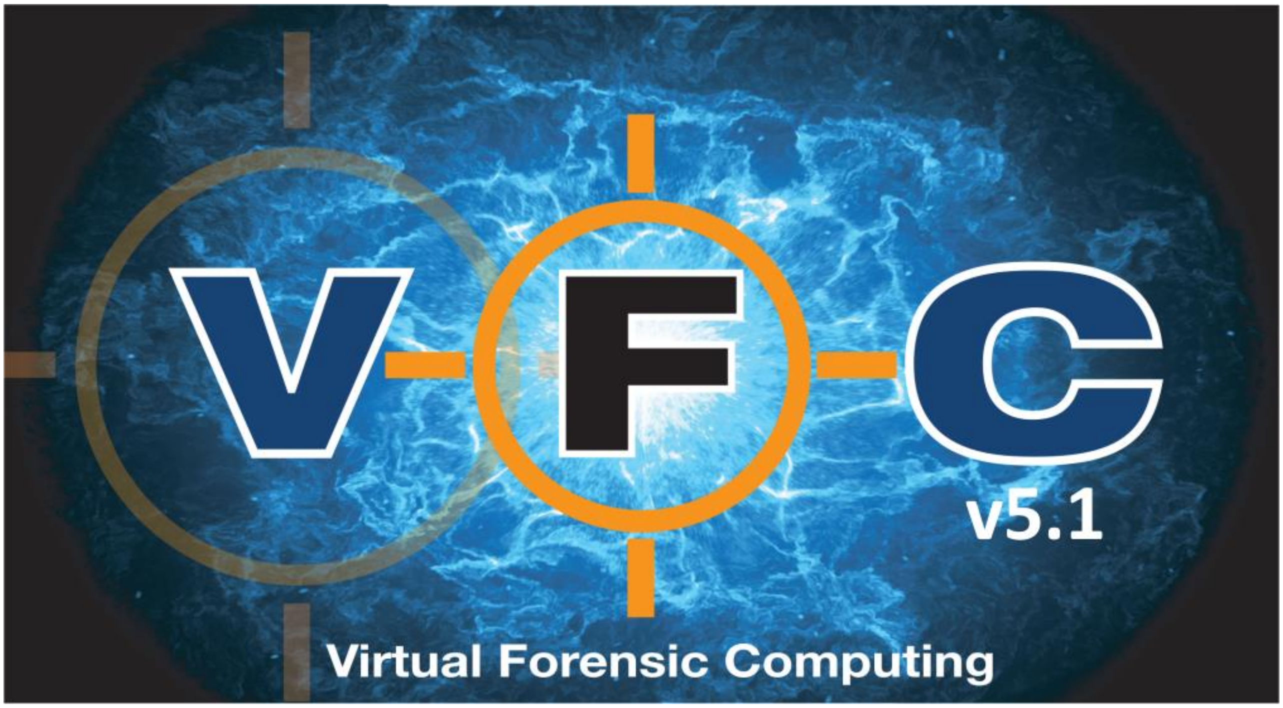


VFC User Guide v5.1

VFC is a registered trademark of MD5 Ltd

Acknowledgements

All rights reserved.

The information in this document is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by MD5 Ltd.

MD5 Ltd assumes no responsibility or liability for any errors or inaccuracies that may appear in this document.

The software described in this document is provided under license on a subscription basis and may only be used or copied in accordance with the terms of such license. VFC will cease to function once the subscription period expires.

VFC® and the V-F-C logo are registered trademarks of MD5 Ltd.

VMware® is a trademark of VMware, Inc. and may be registered in certain jurisdictions.

Microsoft® and Microsoft® Windows® are trademarks of Microsoft Corporation that may be registered in certain jurisdictions.

All other products or name brands are trademarks of their respective holders and are acknowledged.

Contact Details

Address: MD5 Ltd, PO Box 96, Normanton, West Yorkshire, WF6 1WY, United Kingdom
Phone: +44 (0) 1924 220 999
Sales: sales@md5.uk.com
Support: vfc.uk.com/support

Table of Contents

VFC Overview

Welcome to the VFC User Guide. This document explains the purpose of VFC and how to use it. Please see the separate VFC Installation Guide for installation instructions and the FAQ for answers to common questions and troubleshooting suggestions.

Background

VFC is used by digital forensic investigators to create a virtual copy of a suspect computer. The process is forensically safe and does not modify any original evidential data. This procedure allows the investigator to experience the original desktop environment just like the original user. This puts the investigator "in the room" with the suspect, providing invaluable access to software and data that cannot be easily found with a typical "dead box" examination.

In some cases, an experienced investigator could manually perform some of the processes performed by VFC. However, this would be time-consuming and error-prone. VFC automates the process and applies almost 15 years of acquired knowledge to fix numerous known issues and quickly produce a compatible and stable virtual machine in seconds. VFC removes the guesswork from virtualisation and allows the investigator to concentrate on the investigation.

VFC is typically used with a forensic "image" that has been previously created from a physical disk. The use of images is a standard industry practice that ensures the continuity of evidence and avoids the possibility of damaging or contaminating original evidence. VFC can also be used with a physical disk drive. However, in this case, we would strongly recommend that it is connected via a forensic "write blocker" to ensure that no changes are made to the original material.

VFC is compatible with a range of common image "mount" tools and also ships with a built-in mount tool called VFC Mount. This supports the following common image formats:

- .e01
- .ex01
- .aff4
- .vmdk
- Raw / spanned image e.g. .dd, .img, .bin, .raw, .001 etc.

VFC works by creating a temporary disk cache and directing all subsequent reads and writes 'through' this cache. This emulates normal read/write behaviour and allows the guest operating system and installed software to function normally. This process is forensically safe and no changes are made to the original image files or disk.

Advanced Features

VFC has many advanced features not found in other tools. These are built on over 10 years of research and development. The software detects and fixes a large number of potential compatibility issues to maximise the chance of producing a viable virtual machine. VFC is expected to work over 95% of the time but may fail if the system configuration is particularly unusual or there were serious problems on the original hardware before the system was imaged and then virtualised. In these cases, we publish a variety of tips and workaround in the VFC FAQ and provide a comprehensive technical support service if required.

Advanced VFC features include:

- Automatic detection and correction of disk geometry issues
- Automatic target OS detection from Windows 3.1 to Windows 10
- Support for Linux, Sun Solaris and other UEFI based operating systems (some experimental)
- Detection of Windows OS details such as last boot time, user names and password hashes
- Support for SCSI, IDE and SATA mass storage controllers
- Numerous compatibility fixes for problem hardware, drivers, software and OEM utilities
- Windows password bypass disables password validation (now with fuzzy logic)
- Generic password reset allows access to “live” accounts and resets passwords
- Built-in mount tool with specific VMware compatibility features
- Integration third-party forensic analysis tools including EnCase and X-Ways Forensics
- Rapid analysis and VM creation (typically ~ 1 minute)

Basic Workflow

VFC can be used in a variety of ways. The basic process is very quick and simple:

- Mount the evidence file using mount tool (or attach a [write-blocked] physical disk)
- Select the disk and then the relevant partition
- Generate the machine and launch it with VMware

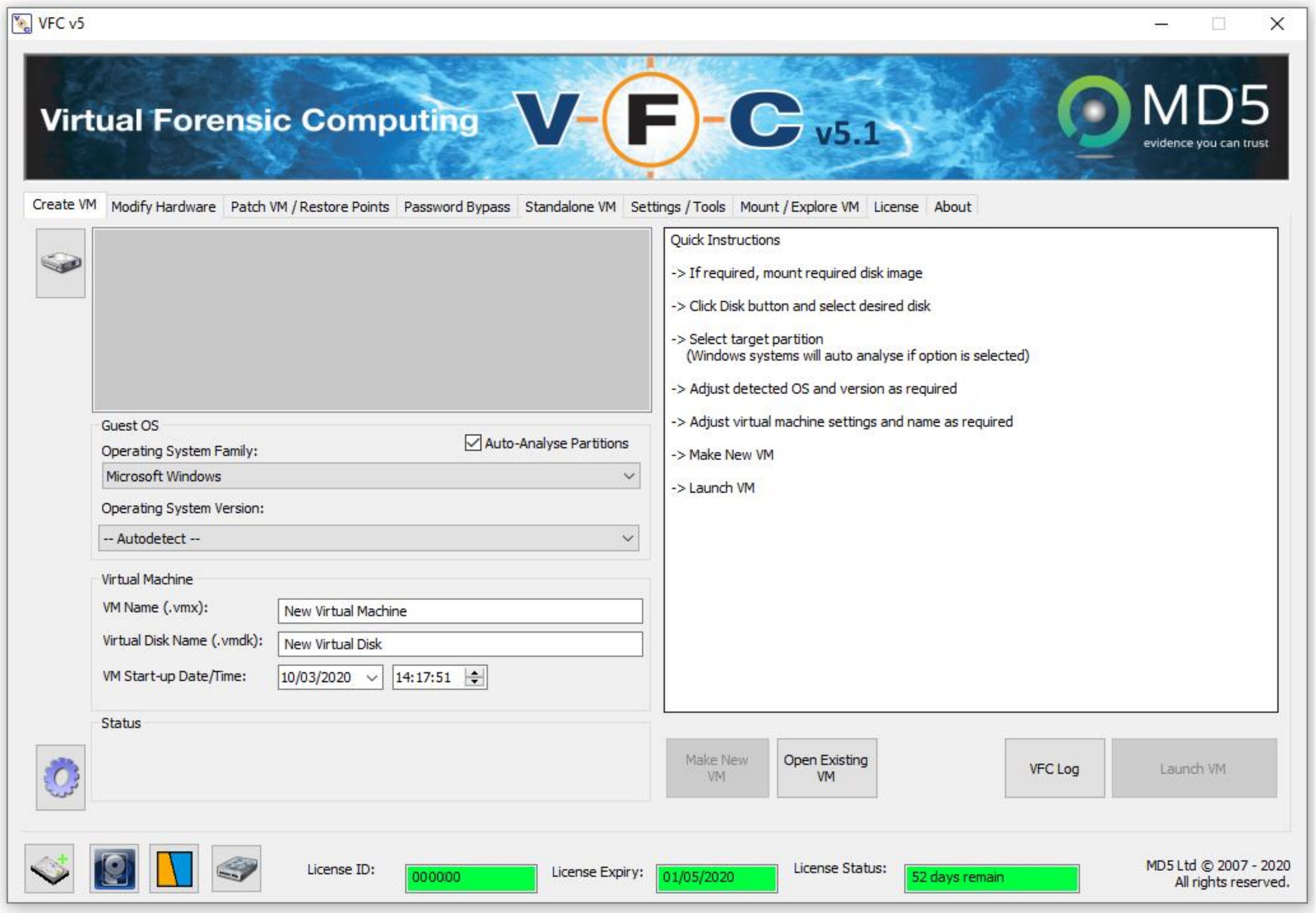
This document explains how to use VFC in a variety of different scenarios. Please see the separate VFC Installation Guide for installation instructions and the FAQ for answers to common questions and troubleshooting suggestions.

VFC License Manager

The VFC License Manager tool can be used to check and upgrade your current VFC license. Please see the VFC FAQ for instructions on how to use License Manager.

The VFC User Interface

The VFC user interface is simple and easy to navigate. It consists of several tabs along the top providing quick access to different feature areas. The majority of day-to-day tasks can be performed using just the "Create VM" tab:



Operating System Family: Microsoft Windows

☑ Auto-Analyse Partitions

Operating System Version: -- Autodetect --

VM Name (.vmx): New Virtual Machine

Virtual Disk Name (.vmdk): New Virtual Disk

VM Start-up Date/Time: 10/03/2020 14:17:51

Quick Instructions

-> If required, mount required disk image

-> Click Disk button and select desired disk

-> Select target partition
(Windows systems will auto analyse if option is selected)

-> Adjust detected OS and version as required

-> Adjust virtual machine settings and name as required

-> Make New VM

-> Launch VM

License ID: 000000 License Expiry: 01/05/2020 License Status: 52 days remain

MD5 Ltd © 2007 - 2020
All rights reserved.

The tabs have the following functions:

- **Create VM** – Analyse and create a virtual machine from image/disk
- **Modify Hardware** – Modify virtual machine hardware such as add disks or enable networking
- **Patch VM / Restore Points** – Used to re-patch an existing VM or one that has been temporarily broken by using the Windows System Restore Point feature
- **Password Bypass** – Disable password authentication on a variety of Windows VMs
- **Standalone VM** – Create a standalone copy of VM for use without VFC
- **Settings / Tools** – Configure VFC / Windows features
- **Mount / Explore VM** – Mount a VM and access its file system
- **License** – Display VFC end user license agreement (EULA)
- **About** – VFC version information and quick access to PDF guides and updates

VFC: Step-by-Step

Mount a forensic whole disk image

The first VFC task is typically to mount the forensic “image” that you wish to analyse. Mounting the image makes it appear to the host system, VFC and VMware that it is connected as a “real” physical disk. In most cases, with industry-standard image formats such as .E01, .Ex01 and .AFF4, this process is forensically safe and does not alter the original image. We recommend taking additional care with other image formats, such as .VMDK, .VHD and .DD that were not originally designed for forensic use. These formats can be used safely provided they are mounted “read-only”.

VFC can be used with a variety of different mount tools. These can be useful to extend the number of formats supported and allow VFC to be used in many creative ways. VFC has been successfully used with the following:

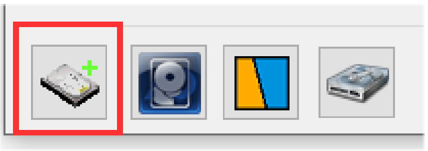
- Mount Image Pro v5/6
- FTK Imager v4.x
- OSF Mount v3
- Guidance Software Encase PDE (Physical Disk Emulator)
- Arsenal Imager Mount (AIM) v3.x

VFC is supplied with a built-in mount tool called **VFC Mount**. This tool supports forensically safe, read-only, mount of common image formats such as: .eE01, .Ex01, .AFF4, .VMDK. It also supports Raw / spanned image formats including: .DD, .IMG, .BIN, and .RAW. We recommend using VFC Mount if possible. We have optimised VFC Mount for use with VMware and it includes several features to maximise compatibility and to avoid common problems

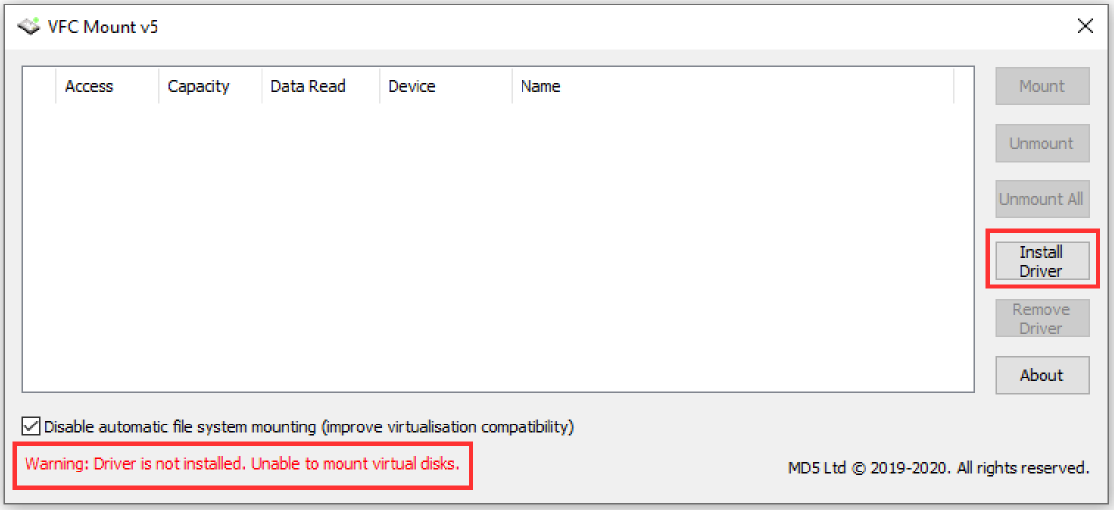
Using VFC Mount

To use VFC Mount for the first time:

1. Launch **VFC Mount** using the icon located at the bottom right of the VFC screen:



2. If this is the first time you have used VFC Mount, it may be necessary to install the mount driver. This is indicated by the red text “Warning: Driver is not installed”



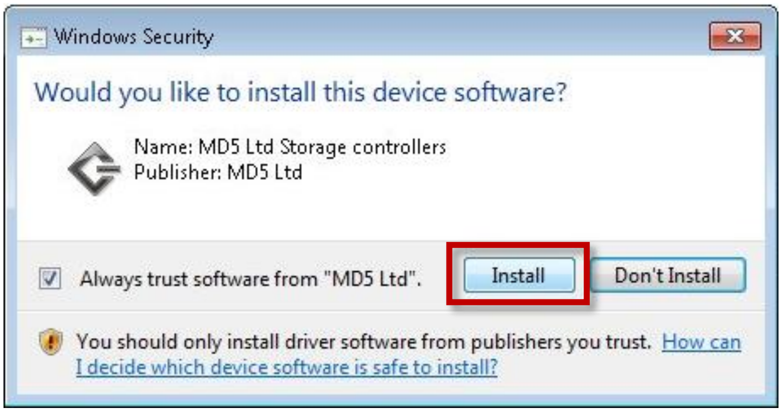
☑ Disable automatic file system mounting (improve virtualisation compatibility)

Warning: Driver is not installed. Unable to mount virtual disks.

MD5 Ltd © 2019-2020. All rights reserved.

3. Click **Install Driver** to install the driver

4. If prompted, click **Install** (see screenshot) to authorise driver installation



Would you like to install this device software?

Name: MD5 Ltd Storage controllers
Publisher: MD5 Ltd

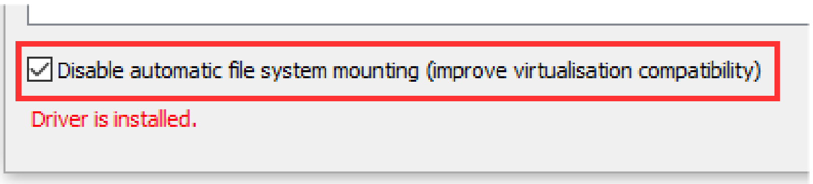
☑ Always trust software from "MD5 Ltd".

You should only install driver software from publishers you trust. How can I decide which device software is safe to install?

TIP: This procedure is typically only required the first time VFC Mount is used or following the installation of a significant new version. Please note that regardless of the installed version of VFC, the 32-bit version of VFC Mount must be used on 32-bit systems and the 64-bit version of VFC Mount must be used on 64-bit systems. VFC automatically loads the correct version.

Disable Windows automatic file system mounting

Before using VFC Mount for the first time, we recommend checking the box to disable Windows automatic file system mounting. This will prevent Windows "locking" images as they are mounted and greatly reduce compatibility problems with VMware:



☑ Disable automatic file system mounting (improve virtualisation compatibility)

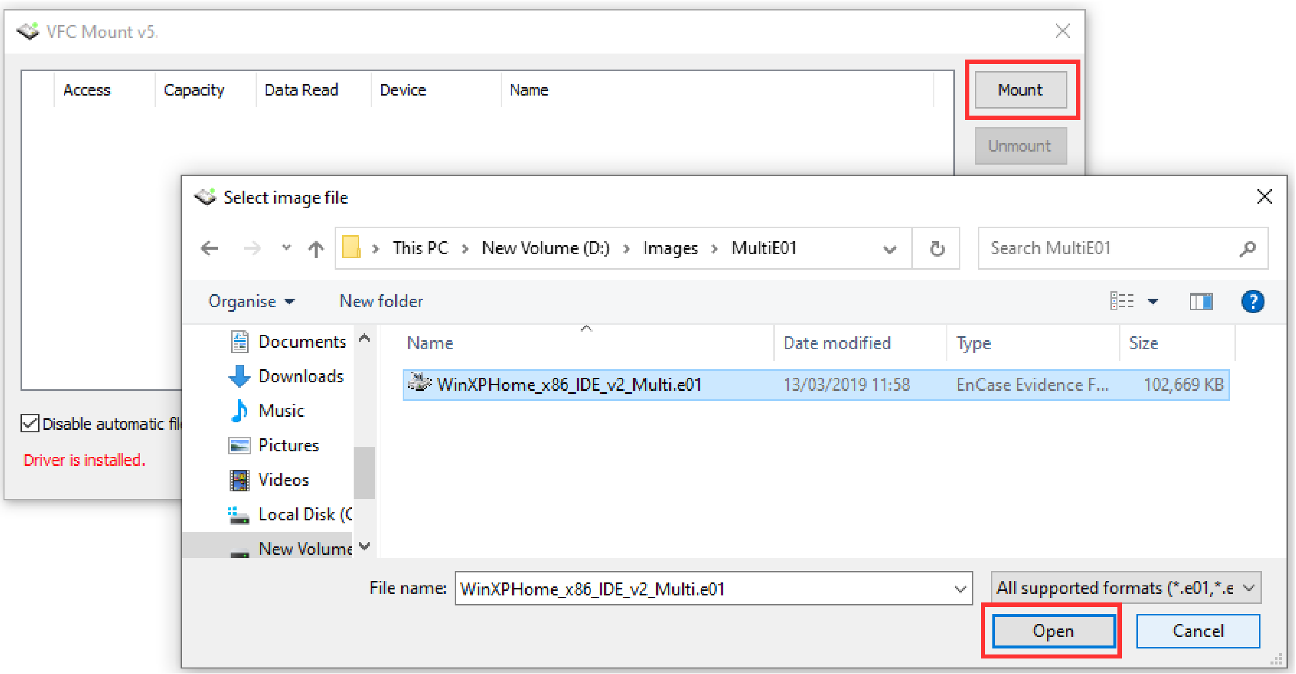
Driver is installed.

Note: This feature means that Windows will not automatically allocate a drive letter for disks/images that are mounted in future. If you need this behaviour again, simply untick the box again or manually assign a drive letter using the Windows Disk Manager tool.

Mounting a Drive with VFC Mount

To mount an image with VFC Mount, proceed as follows:

1. Click **Mount**
2. Browse to the folder containing the desired image
3. Select the image
4. Click **Open**



Access	Capacity	Data Read	Device	Name

☑ Disable automatic fil

Driver is installed.

This PC › New Volume (D:) › Images › MultiE01

Search MultiE01

Name	Date modified	Type	Size
WinXPHome_x86_IDE_v2_Multi.e01	13/03/2019 11:58	EnCase Evidence F...	102,669 KB

File name: WinXPHome_x86_IDE_v2_Multi.e01

All supported formats (*.e01,*.e

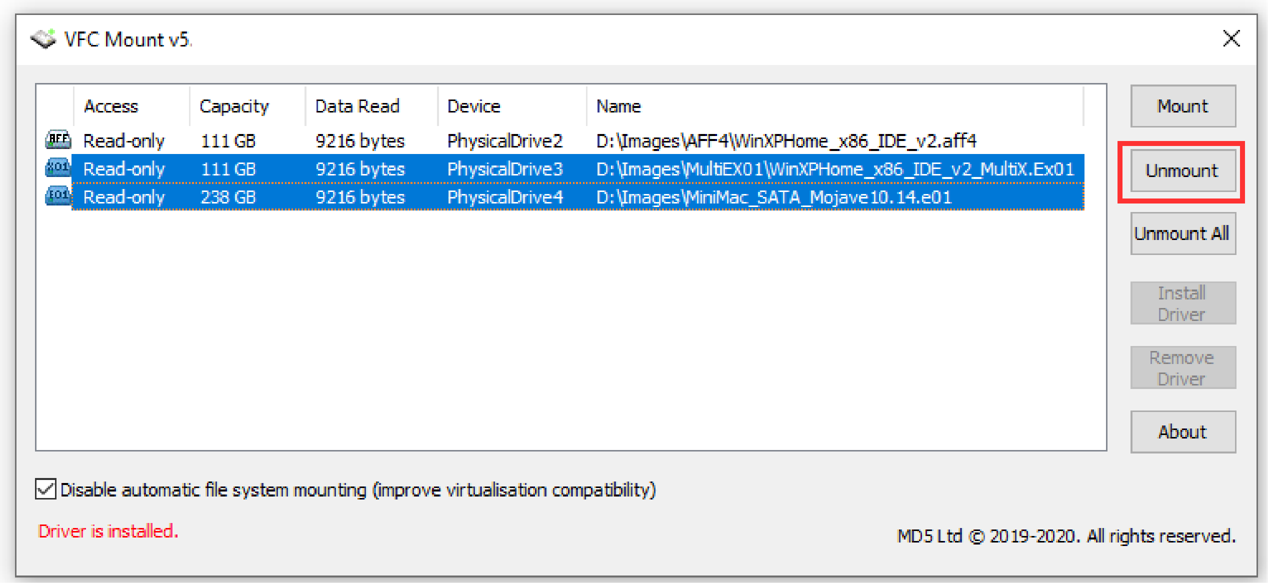
Mounting Multiple Images

If necessary, you can mount multiple images with VFC Mount. To do this, simply click Mount again and select the desired image. This technique may be necessary when virtualising systems that had multiple physical disks installed.

TIP: We recommend mounting all applicable images before using VFC to create a virtual machine.

Unmounting Images

Once you are finished with a mounted drive, simply highlight the no-longer-required images and click **Unmount**. If necessary, you can select multiple drives by using **Control**+**Shift**:



VFC Mount v5.

Access	Capacity	Data Read	Device	Name
Read-only	111 GB	9216 bytes	PhysicalDrive2	D:\Images\AFF4\WinXPHome_x86_IDE_v2.aff4
Read-only	111 GB	9216 bytes	PhysicalDrive3	D:\Images\MultiEX01\WinXPHome_x86_IDE_v2_MultiX.Ex01
Read-only	238 GB	9216 bytes	PhysicalDrive4	D:\Images\MiniMac_SATA_Mojave10.14.e01

☑ Disable automatic file system mounting (improve virtualisation compatibility)

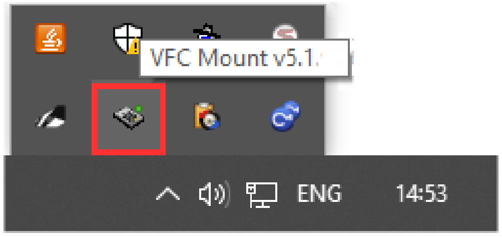
Driver is installed.

MD5 Ltd © 2019-2020. All rights reserved.

TIP: Please remember that when you unmount an image it is equivalent to unplugging a physical disk. Any running VM that is using that image will immediately fail. We recommend you leave images mounted until all VMs are closed. It is not necessary to unmount images before shutting down the workstation; this will happen automatically when you log out of Windows.

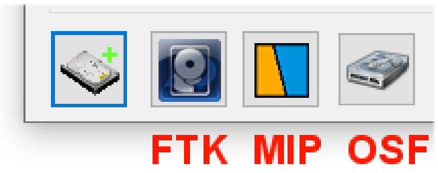
Closing VFC Mount

VFC Mount runs in the background and is independent of the VFC application. This is required to ensure that images remain mounted whilst they are used in VMware. To access VFC Mount again, simply click on the icon in the system notification (tray) area:



Mounting a Disk with External Mounting Tools

VFC provides icons to launch common mount tools. This currently supports FTK Imager (FTK), Mount Image Pro (MIP) and OSFMount v3 (OSF). These "quick launch" icon(s) will appear in the bottom left of the VFC application when the associated third-party applications are installed:



Tips for using FTK Imager

We recommend the following configuration when using FTK Imager with VFC:

- Mount physical only (not logical)
- Block device / read-only

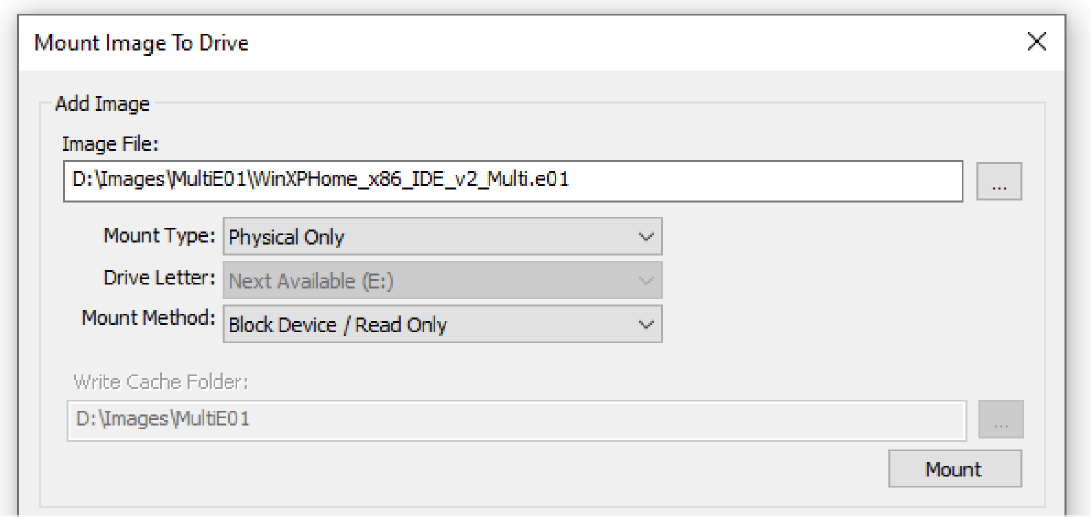


Image File: D:\Images\MultiE01\WinXPHome_x86_IDE_v2_Multi.e01

Mount Type: Physical Only

Drive Letter: Next Available (E:)

Mount Method: Block Device / Read Only

Write Cache Folder: D:\Images\MultiE01

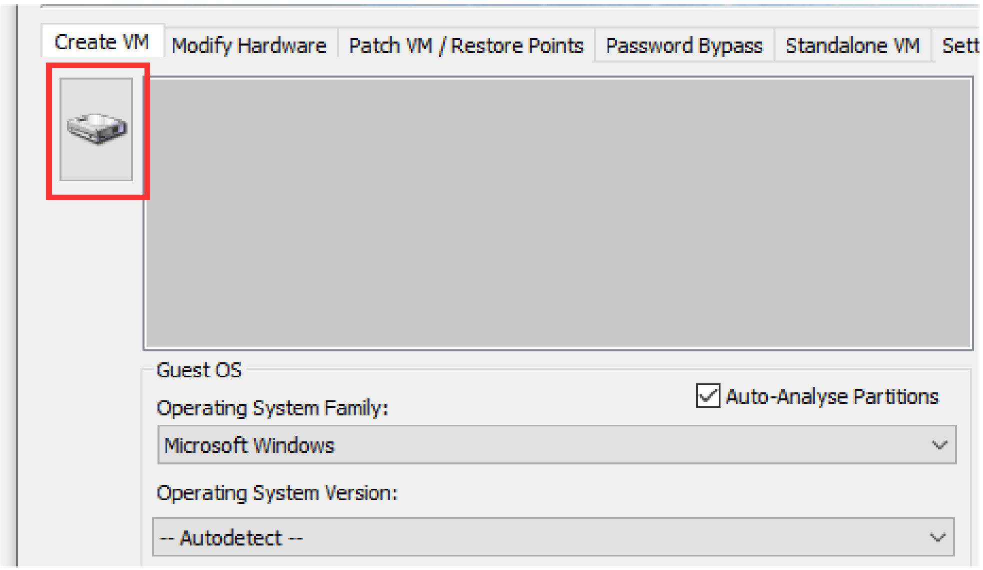
TIP *If using either Encase PDE or the FTK Imager mount function, closing either of these applications will cause the image to dismount. The MIP GUI can be closed but will minimise the application to the system tray whilst maintaining the mounted status of the image, similar to the behaviour of VFC Mount, as described in the section above.*

NB2 *If you need to select the OS folder using the Options screen in VFC you may need to mount the drive as Physical AND Logical.*

Enumerating mounting drives (Selecting source drive)

Once the desired forensic images have been mounted, the next task is typically to identify the drive to VFC. To do this, proceed as follows:

1. Click the **Enumerate Drives** icon:



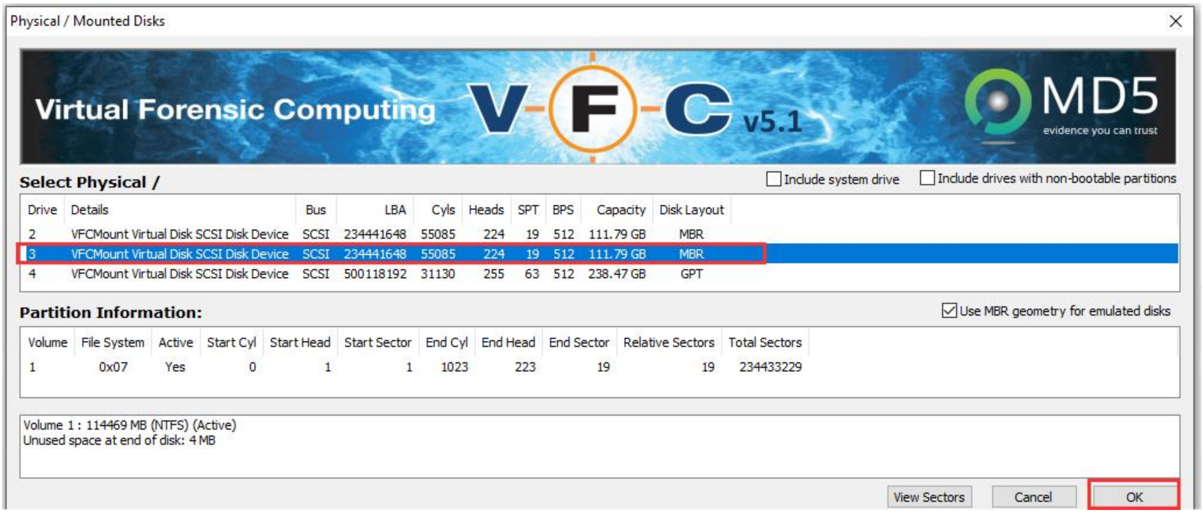
Guest OS

☑ Auto-Analyse Partitions

Operating System Family: Microsoft Windows

Operating System Version: -- Autodetect --

2. Select the desired (emulated) drive:



Select Physical /

□ Include system drive □ Include drives with non-bootable partitions

Drive	Details	Bus	LBA	Cyls	Heads	SPT	BPS	Capacity	Disk Layout
2	VFCMount Virtual Disk SCSI Disk Device	SCSI	234441648	55085	224	19	512	111.79 GB	MBR
3	VFCMount Virtual Disk SCSI Disk Device	SCSI	234441648	55085	224	19	512	111.79 GB	MBR
4	VFCMount Virtual Disk SCSI Disk Device	SCSI	500118192	31130	255	63	512	238.47 GB	GPT

Partition Information:

☑ Use MBR geometry for emulated disks

Volume	File System	Active	Start Cyl	Start Head	Start Sector	End Cyl	End Head	End Sector	Relative Sectors	Total Sectors
1	0x07	Yes	0	1	1	1023	223	19	19	234433229

Volume 1 : 114469 MB (NTFS) (Active)
Unused space at end of disk: 4 MB

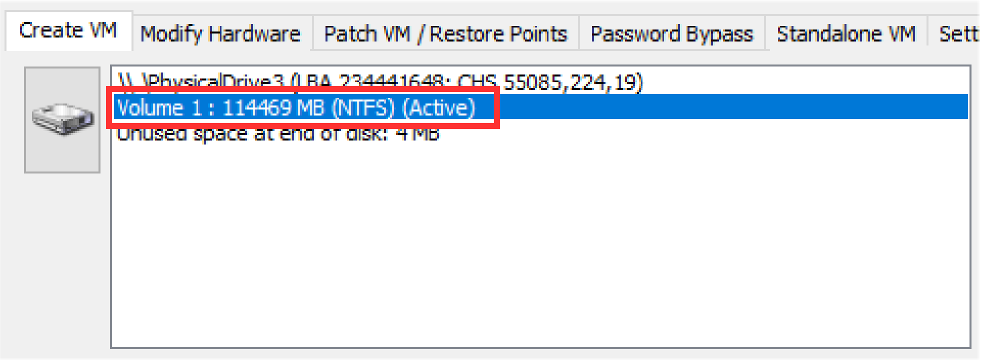
3. Click **OK**

TIP: Rarely, you may need to reboot the forensic workstation and remount the drive before it is visible to VFC. This happens when Windows ceases to notice new disks have been mounted and can happen after a large number of disk images have been mounted/dismounted.

Selecting target partition / file system

Once the desired drive has been selected, proceed as follows to select a system partition to analyse. In most scenarios, the desired partition will be the largest one and may be marked "Active":

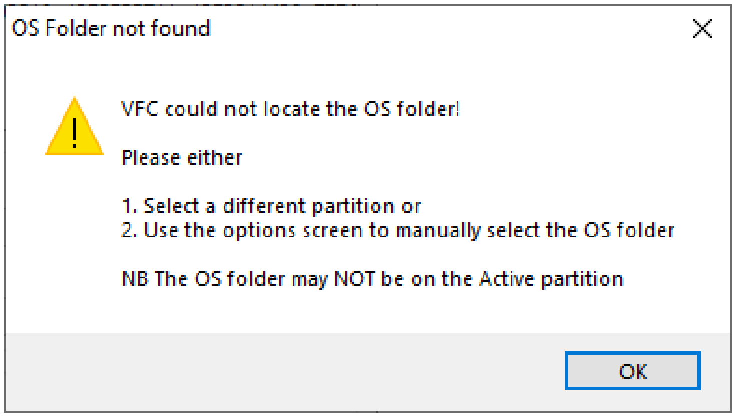
1. Click the desired partition/volume:



\\.\PhysicalDrive3 (LBA 234441648; CHS 55085,224,19)
Volume 1 : 114469 MB (NTFS) (Active)
Unused space at end of disk: 4 MB

2. Wait for VFC to analyse the file system. This will typically take a few seconds.

3. In some cases, VFC may not recognize the guest operating system. This can happen if you select the wrong partition. In this case, please first check the target partition is correct and if necessary, try again:



OS Folder not found

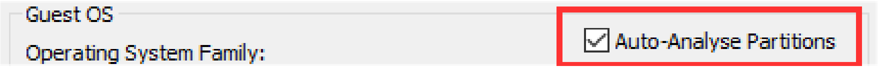
VFC could not locate the OS folder!

Please either

1. Select a different partition or
2. Use the options screen to manually select the OS folder

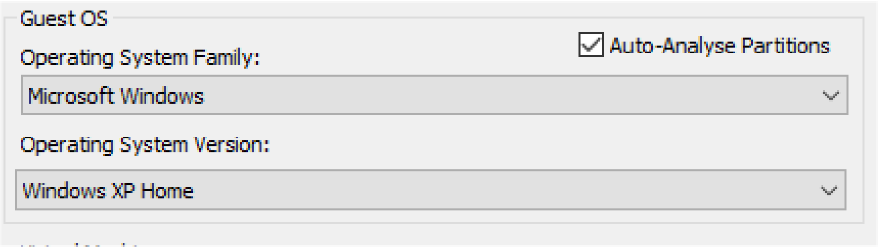
NB The OS folder may NOT be on the Active partition

4. Alternatively, try unticking **Auto-Analyse partitions** and try again:



Guest OS
Operating System Family:
☑ Auto-Analyse Partitions

5. For most Windows guest operating systems, VFC will automatically detect the OS version and configuration. The detected OS/edition is displayed beneath the list of file systems. If the selected configuration is incorrect, please amend it before proceeding further:



Guest OS

Operating System Family: Microsoft Windows

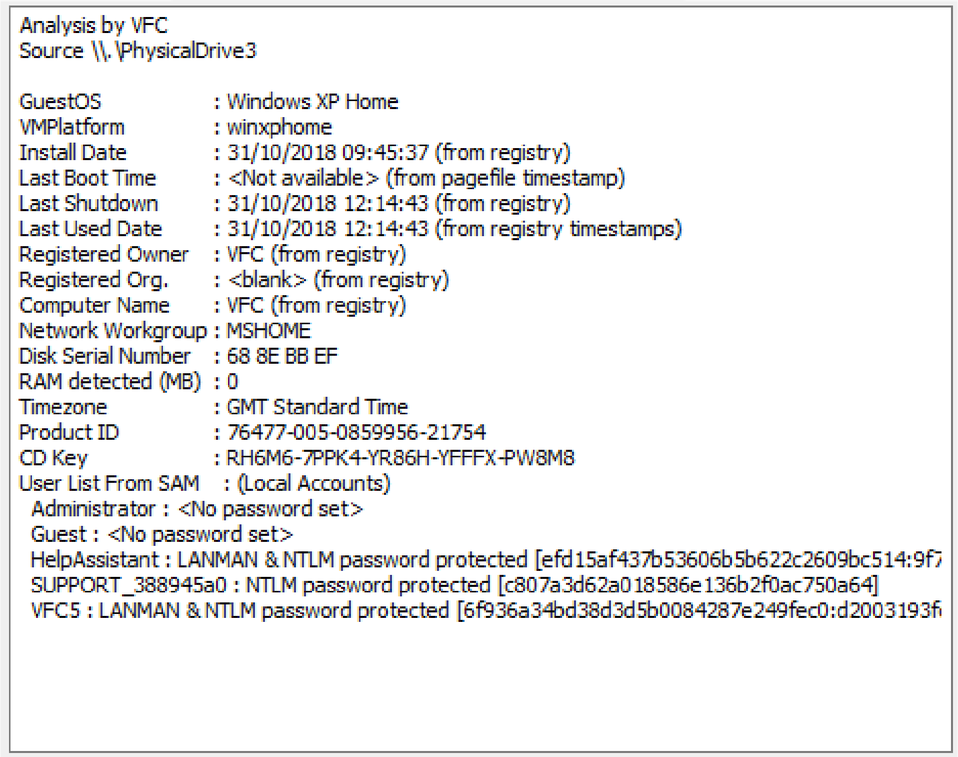
☑ Auto-Analyse Partitions

Operating System Version: Windows XP Home

TIP: VFC may not recognize the specific version of Linux / UEFI-*based operating system. In this case, please use the drop-down boxes to select the closest match possible. It is not necessary to have an exact match but please ensure you select the correct platform as either 32-bit or 64-bit.*

TIP: It is not essential that VFC recognize the specific OS version. In many scenarios, the built-in fallback behaviour of VFC will still result in a viable virtual machine. The process is very quick and it should not take very long to find a configuration that works.

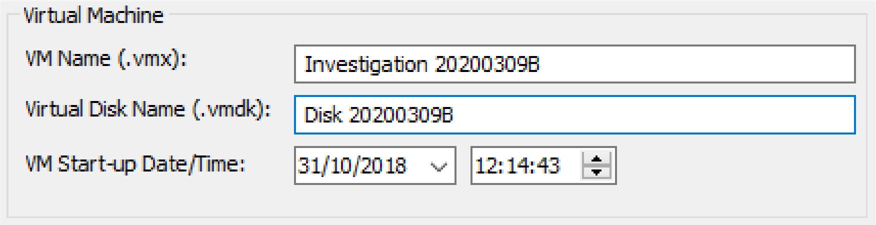
6. For many common operating systems, VFC will be able to detect specific operating system parameters. Depending on the scenario, this may include the OS name, last boot/shutdown/used time, registered own, time zone, user names and in some cases password hashes:



```
Analysis by VFC
Source \\.\PhysicalDrive3

GuestOS              : Windows XP Home
VMPlatform           : winxphome
Install Date         : 31/10/2018 09:45:37 (from registry)
Last Boot Time       : <Not available> (from pagefile timestamp)
Last Shutdown        : 31/10/2018 12:14:43 (from registry)
Last Used Date       : 31/10/2018 12:14:43 (from registry timestamps)
Registered Owner     : VFC (from registry)
Registered Org.      : <blank> (from registry)
Computer Name        : VFC (from registry)
Network Workgroup : MSHOME
Disk Serial Number   : 68 8E BB EF
RAM detected (MB)  : 0
Timezone             : GMT Standard Time
Product ID           : 76477-005-0859956-21754
CD Key               : RH6M6-7PPK4-YR86H-YFFFX-PW8M8
User List From SAM     : (Local Accounts)
  Administrator : <No password set>
  Guest : <No password set>
  HelpAssistant : LANMAN & NTLM password protected [efd15af437b53606b5b622c2609bc514:9f7
  SUPPORT_388945a0 : NTLM password protected [c807a3d62a018586e136b2f0ac750a64]
  VFC5 : LANMAN & NTLM password protected [6f936a34bd38d3d5b0084287e249fec0:d2003193f
```

TIP: This Target System Information (TSI) may be valuable in an investigation. For instance, the last shutdown time may indicate if the system was in use at a time of interest and the user names indicate who regularly used the computer or give password clues. The password hashes may be used to "crack" the password and gain access to both the system and other software secured with the same password. VFC embeds this information into both the VFC log file and the VM configuration file so that it is visible within VMware. It can also easily be copied from VFC into a forensic examination report. Please see below for an example of using the password hashes.

7. When you have determined that the OS detection is correct, enter a suitable VM name and disk name:



Virtual Machine

VM Name (.vmx): Investigation 20200309B

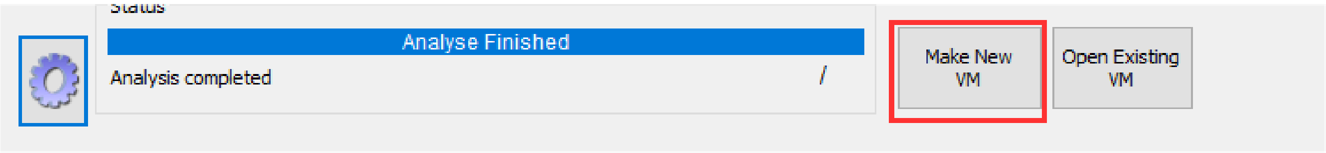
Virtual Disk Name (.vmdk): Disk 20200309B

VM Start-up Date/Time: 31/10/2018 12:14:43

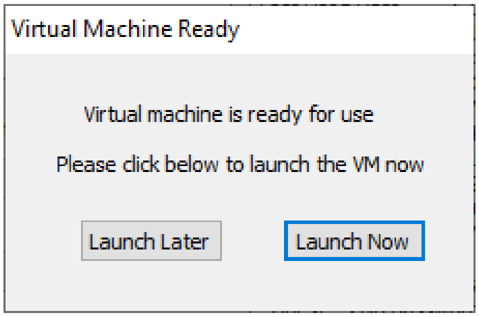
TIP: You can also adjust the VM start-up date/time. Initially, this is set to the time that the guest OS last shutdown. However, it may be desirable to set this to a previous time. For instance, this can be used to gain access to time-limited software.

8. If necessary, additional VM creation settings may be configured by clicking the **Options** (cog) icon. These are explained in more detail later in this guide. ⚙

9. Click **Make New VM** and follow the on-screen prompts to create the virtual machine:



10. Finally, click **Launch Now** to start the VM immediately in VMware:


Virtual Machine Ready

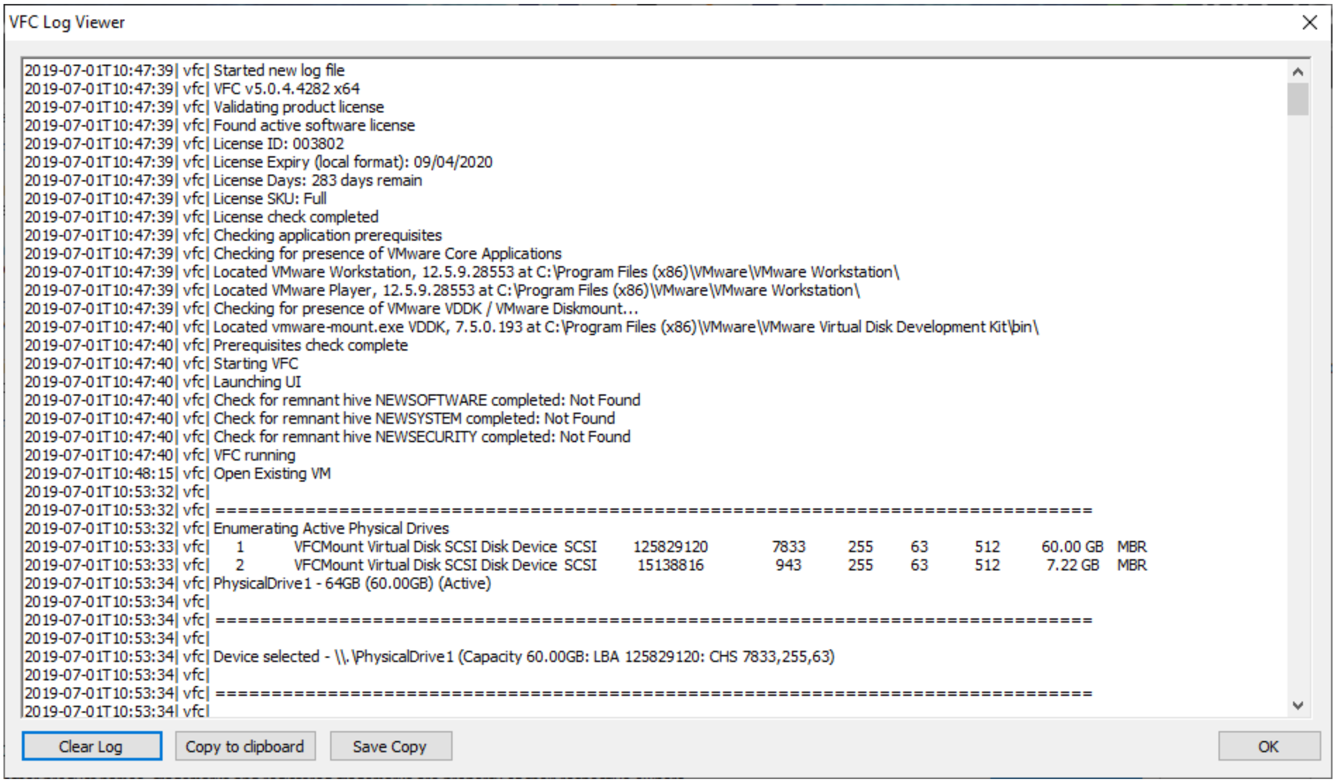
Virtual machine is ready for use

Please click below to launch the VM now

The VFC Log File

For each session of VFC, a log file is created that records details about the host system, guest OS details, connected drives and VFC configuration. This information can be included in a forensic report and, if necessary, used to replicate the process used to generate the virtual machine.

The log file can act as contemporaneous notes, to support an investigation and can also help with validation and verification for the international laboratory standard, ISO 17025. The log file records each step of the VFC process with time and date stamps, (from the host system). We recommend saving a copy of the Log file for each VFC VM generated:



VFC Log Viewer

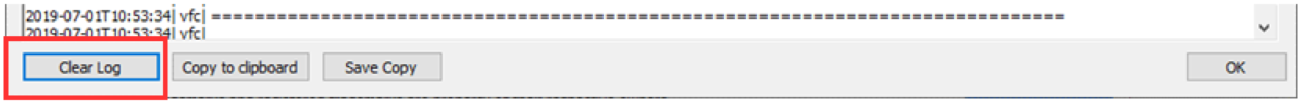
```
2019-07-01T10:47:39| vfc| Started new log file
2019-07-01T10:47:39| vfc| VFC v5.0.4.4282 x64
2019-07-01T10:47:39| vfc| Validating product license
2019-07-01T10:47:39| vfc| Found active software license
2019-07-01T10:47:39| vfc| License ID: 003802
2019-07-01T10:47:39| vfc| License Expiry (local format): 09/04/2020
2019-07-01T10:47:39| vfc| License Days: 283 days remain
2019-07-01T10:47:39| vfc| License SKU: Full
2019-07-01T10:47:39| vfc| License check completed
2019-07-01T10:47:39| vfc| Checking application prerequisites
2019-07-01T10:47:39| vfc| Checking for presence of VMware Core Applications
2019-07-01T10:47:39| vfc| Located VMware Workstation, 12.5.9.28553 at C:\Program Files (x86)\VMware\VMware Workstation\
2019-07-01T10:47:39| vfc| Located VMware Player, 12.5.9.28553 at C:\Program Files (x86)\VMware\VMware Workstation\
2019-07-01T10:47:39| vfc| Checking for presence of VMware VDDK / VMware Diskmount...
2019-07-01T10:47:40| vfc| Located vmware-mount.exe VDDK, 7.5.0.193 at C:\Program Files (x86)\VMware\VMware Virtual Disk Development Kit\bin\
2019-07-01T10:47:40| vfc| Prerequisites check complete
2019-07-01T10:47:40| vfc| Starting VFC
2019-07-01T10:47:40| vfc| Launching UI
2019-07-01T10:47:40| vfc| Check for remnant hive NEWSOFTWARE completed: Not Found
2019-07-01T10:47:40| vfc| Check for remnant hive NEWSYSTEM completed: Not Found
2019-07-01T10:47:40| vfc| Check for remnant hive NEWSECURITY completed: Not Found
2019-07-01T10:47:40| vfc| VFC running
2019-07-01T10:48:15| vfc| Open Existing VM
2019-07-01T10:53:32| vfc|
2019-07-01T10:53:32| vfc| ===========================================================================
2019-07-01T10:53:32| vfc| Enumerating Active Physical Drives
2019-07-01T10:53:33| vfc|    1      VFCMount Virtual Disk SCSI Disk Device  SCSI    125829120      7833    255    63     512     60.00 GB  MBR
2019-07-01T10:53:33| vfc|    2      VFCMount Virtual Disk SCSI Disk Device  SCSI     15138816       943    255    63     512      7.22 GB  MBR
2019-07-01T10:53:34| vfc| PhysicalDrive1 - 64GB (60.00GB) (Active)
2019-07-01T10:53:34| vfc|
2019-07-01T10:53:34| vfc| ===========================================================================
2019-07-01T10:53:34| vfc|
2019-07-01T10:53:34| vfc| Device selected - \\.\PhysicalDrive1 (Capacity 60.00GB: LBA 125829120: CHS 7833,255,63)
2019-07-01T10:53:34| vfc|
2019-07-01T10:53:34| vfc| ===========================================================================
2019-07-01T10:53:34| vfc|
```

TIP: VFC creates one continuous log file for each session. It does not differentiate between cases or virtual machines. You may like to clear the log file before starting a new case.

TIP: The log file is a working document. VFC needs to write to it constantly to maintain the forensic audit trail of what has been done to the target system. If the log file is open, VFC will not work (you'll see a blue circle instead of a cursor). As it says at the foot of the log file, "Please close the log file before continuing to use VFC".

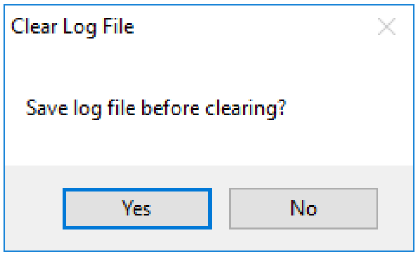
Saving and Clearing the VFC Log File

1. To avoid cross-contamination of data from different cases or VMs, use the **Clear Log File** button:



```
2019-07-01T10:53:34| vfc| ================================================================================
2019-07-01T10:53:34| vfc|
```

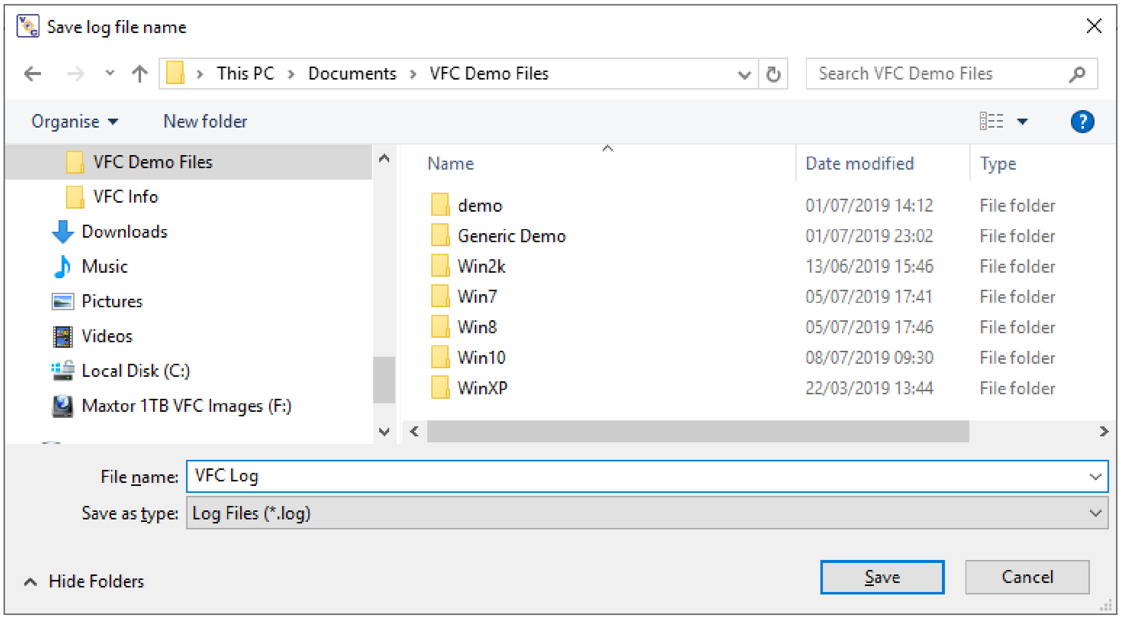
2. You will be asked if you wish to save a copy of the log file (recommended):



Clear Log File

Save log file before clearing?

3. When saving the log, select a target file name:



Save log file name

This PC > Documents > VFC Demo Files

Name	Date modified	Type
demo	01/07/2019 14:12	File folder
Generic Demo	01/07/2019 23:02	File folder
Win2k	13/06/2019 15:46	File folder
Win7	05/07/2019 17:41	File folder
Win8	05/07/2019 17:46	File folder
Win10	08/07/2019 09:30	File folder
WinXP	22/03/2019 13:44	File folder

File name: VFC Log

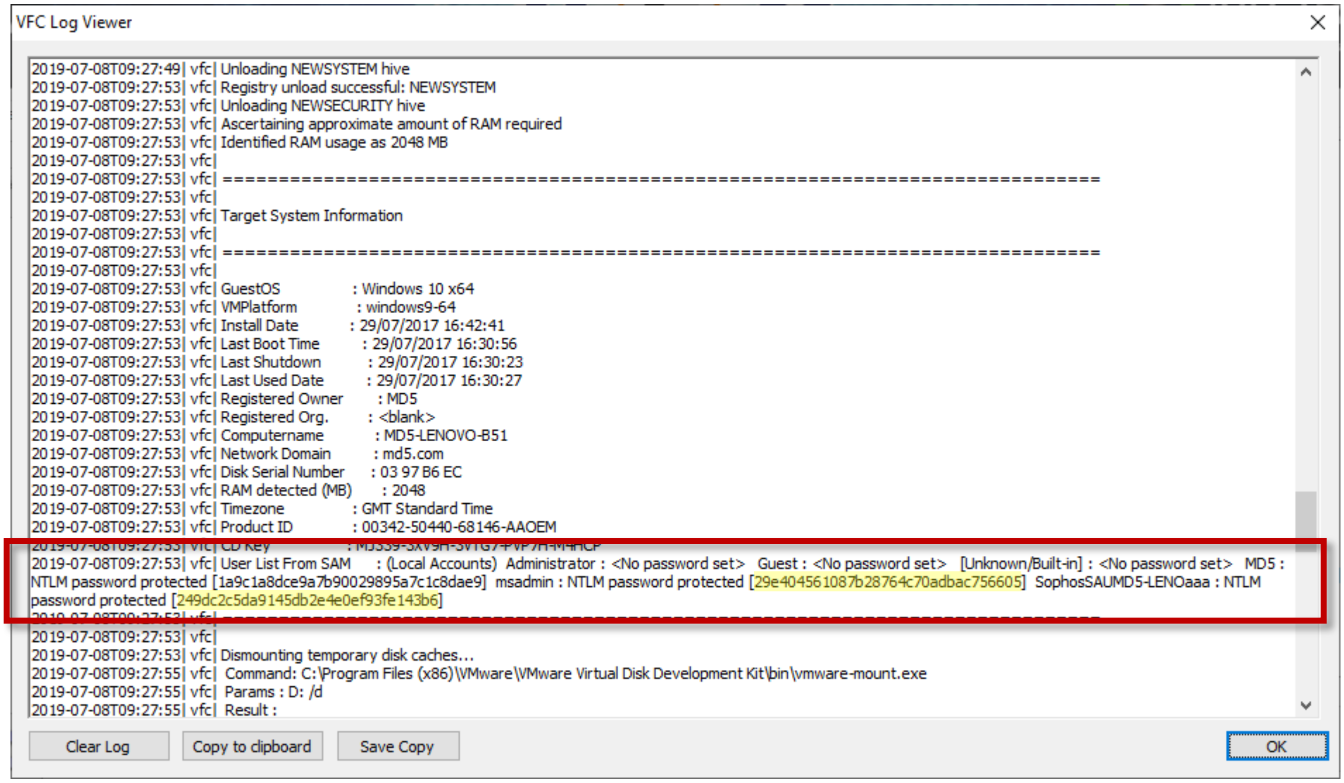
Save as type: Log Files (*.log)

Advanced: Using detected system information to crack account passwords (Target System Information)

Whilst VFC provides two different password bypass techniques, it may sometimes be desirable to access the guest system with the original password. For instance, this can provide access to other software that was secured with the same password or data that was encrypted with the Windows Encrypted File System (EFS). The user name/password may also provide other clues that allow the investigator access to other software and systems used by the same user. In such cases, it may be possible to use the password hashes found by VFC to “crack” the password and gain access.

The password hashes are included in the VFC log file. These can be cracked using “rainbow” tables and online solutions such as *www.hashkiller.co.uk* or the paid-for *www.crackstation.net*. To access the password hashes proceed as follows:

1. Click **VFC Log** (or manually open the log file in Notepad or similar)
2. Scroll down to the **Target System Information** section
3. Locate the desired user account and select the password hash
4. Copy the hash into the tool of choice to crack it



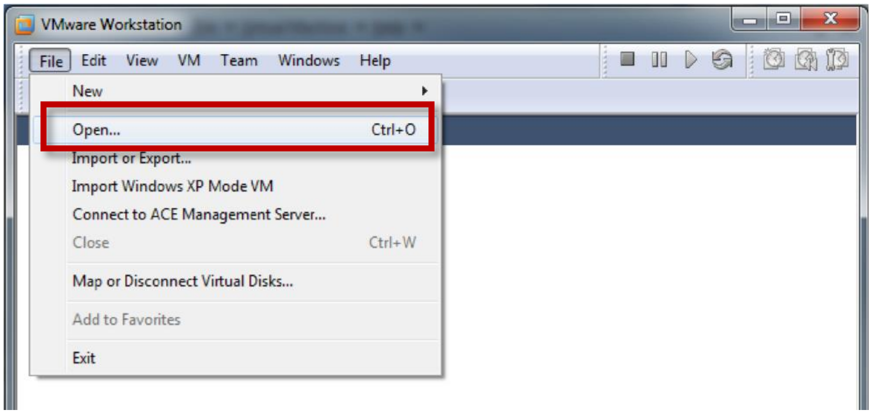
```
2019-07-08T09:27:49| vfc| Unloading NEWSYSTEM hive
2019-07-08T09:27:53| vfc| Registry unload successful: NEWSYSTEM
2019-07-08T09:27:53| vfc| Unloading NEWSECURITY hive
2019-07-08T09:27:53| vfc| Ascertaining approximate amount of RAM required
2019-07-08T09:27:53| vfc| Identified RAM usage as 2048 MB
2019-07-08T09:27:53| vfc|
2019-07-08T09:27:53| vfc| ================================================================================
2019-07-08T09:27:53| vfc|
2019-07-08T09:27:53| vfc| Target System Information
2019-07-08T09:27:53| vfc|
2019-07-08T09:27:53| vfc| ================================================================================
2019-07-08T09:27:53| vfc|
2019-07-08T09:27:53| vfc| GuestOS              : Windows 10 x64
2019-07-08T09:27:53| vfc| VMPlatform            : windows9-64
2019-07-08T09:27:53| vfc| Install Date         : 29/07/2017 16:42:41
2019-07-08T09:27:53| vfc| Last Boot Time        : 29/07/2017 16:30:56
2019-07-08T09:27:53| vfc| Last Shutdown         : 29/07/2017 16:30:23
2019-07-08T09:27:53| vfc| Last Used Date        : 29/07/2017 16:30:27
2019-07-08T09:27:53| vfc| Registered Owner       : MD5
2019-07-08T09:27:53| vfc| Registered Org.       : <blank>
2019-07-08T09:27:53| vfc| Computername          : MD5-LENOVO-B51
2019-07-08T09:27:53| vfc| Network Domain        : md5.com
2019-07-08T09:27:53| vfc| Disk Serial Number    : 03 97 B6 EC
2019-07-08T09:27:53| vfc| RAM detected (MB)      : 2048
2019-07-08T09:27:53| vfc| Timezone             : GMT Standard Time
2019-07-08T09:27:53| vfc| Product ID           : 00342-50440-68146-AAOEM
2019-07-08T09:27:53| vfc| CD Key              : MJ339-3XV9H-3VTG7-PVP7H-M4HCP
2019-07-08T09:27:53| vfc| User List From SAM     : (Local Accounts)  Administrator : <No password set>   Guest : <No password set>   [Unknown/Built-in] : <No password set>   MD5 :
NTLM password protected [1a9c1a8dce9a7b90029895a7c1c8dae9]  msadmin : NTLM password protected [29e404561087b28764c70adbac756605]  SophosSAUMD5-LENOaaa : NTLM
password protected [249dc2c5da9145db2e4e0ef93fe143b6]
2019-07-08T09:27:53| vfc| ================================================================================
2019-07-08T09:27:53| vfc|
2019-07-08T09:27:53| vfc| Dismounting temporary disk caches...
2019-07-08T09:27:55| vfc|  Command: C:\Program Files (x86)\VMware\VMware Virtual Disk Development Kit\bin\vmware-mount.exe
2019-07-08T09:27:55| vfc|  Params : D: /d
2019-07-08T09:27:55| vfc|  Result :
```

Opening the virtual machine directly in VMware

Once VFC has generated the virtual machine, it can be directly opened in VMware. To do this, please proceed as follows:

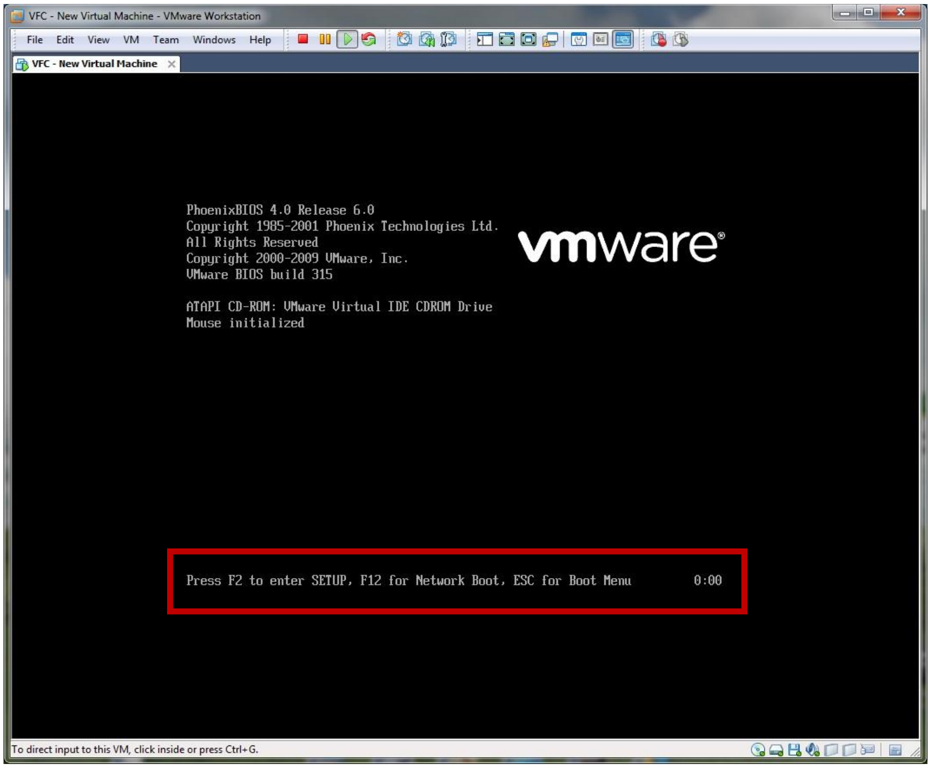
1. Ensure that VMware is launched with Administrator privileges (see above and FAQ)

2. Select **File** / **Open**



3. Click Power On

4. If necessary, press **F2** to access the VMware BIOS setup tool or **Esc** to access the boot menu


VFC - New Virtual Machine - VMware Workstation
File
Edit
View
VM
Team
Windows
Help
VFC - New Virtual Machine
vmware®
To direct input to this VM, click inside or press Ctrl+G.

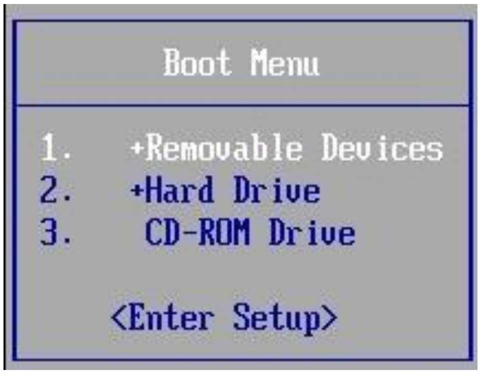
```
PhoenixBIOS 4.0 Release 6.0
Copyright 1985-2001 Phoenix Technologies Ltd.
All Rights Reserved
Copyright 2000-2009 VMware, Inc.
VMware BIOS build 315

ATAPI CD-ROM: VMware Virtual IDE CDROM Drive
Mouse initialized

Press F2 to enter SETUP, F12 for Network Boot, ESC for Boot Menu        0:00
```

Advanced: Changing the VMware boot order

The default boot order is Floppy Disk, Hard Disk then CD-ROM. Typically, the Boot Menu will need to be accessed in circumstances where you wish to boot from a CD or an attached ISO image. It may also be necessary to change the boot order if multiple (virtual) hard disks are present.

To access the VM boot menu, proceed as follows:

1. Start the virtual machine
2. Quickly, click into the virtual machine (so the keyboard input is captured)
3. When prompted, press **F2**
4. Select the desired boot item:

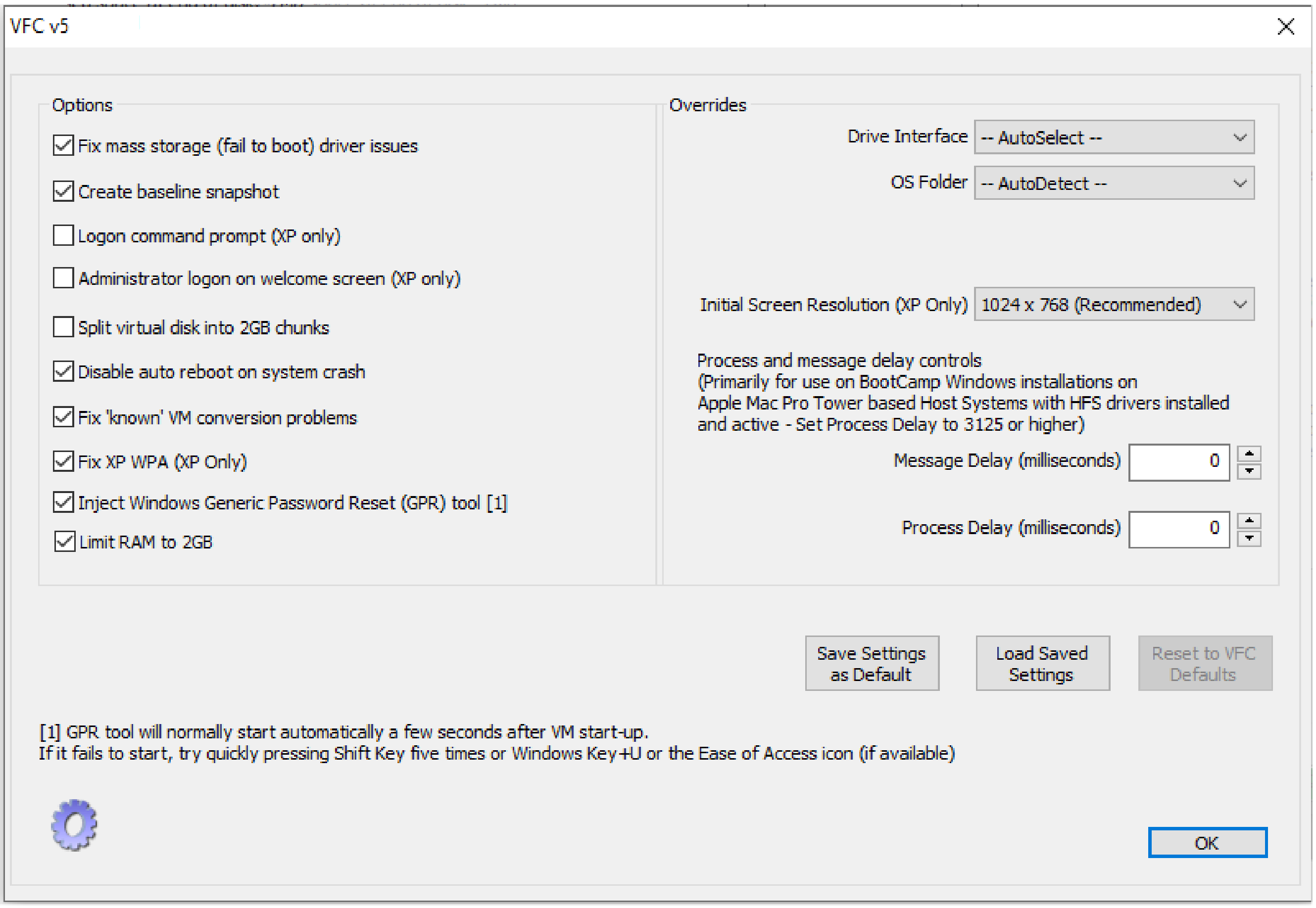


TIP: You can also use the keyboard shortcut "Ctrl + Alt" to switch between inputs. Once you are focused on the VM, access to the virtual keyboard will be enabled and pressing the 'Esc' key will display the Boot Menu. The Keyboard shortcut 'Ctrl + Alt' can also be used to switch between VMware application key-entry (the main VMware window) and interacting with the VM itself.

TIP: VFC will set the boot delay to 3 seconds (3000 milliseconds) to allow easier access to the boot menu. This value can be manually increased further by editing the generated .vmx file and adjusting the 'bios.bootDelay' setting. To allow a 10-second delay, set this value to '10000'.

Changing default behaviour with VFC Options

The VFC Options screen may be opened by click the "cog" icon. This allows advanced features of VFC to be customised. In most cases, these should not need to be changed:



VFC v5

Options

☑ Fix mass storage (fail to boot) driver issues

☑ Create baseline snapshot

□ Logon command prompt (XP only)

□ Administrator logon on welcome screen (XP only)

□ Split virtual disk into 2GB chunks

☑ Disable auto reboot on system crash

☑ Fix 'known' VM conversion problems

☑ Fix XP WPA (XP Only)

☑ Inject Windows Generic Password Reset (GPR) tool [1]

☑ Limit RAM to 2GB

Overrides

Drive Interface: -- AutoSelect --

OS Folder: -- AutoDetect --

Initial Screen Resolution (XP Only): 1024 x 768 (Recommended)

Process and message delay controls
(Primarily for use on BootCamp Windows installations on
Apple Mac Pro Tower based Host Systems with HFS drivers installed
and active - Set Process Delay to 3125 or higher)

Message Delay (milliseconds): 0

Process Delay (milliseconds): 0

[1] GPR tool will normally start automatically a few seconds after VM start-up.
If it fails to start, try quickly pressing Shift Key five times or Windows Key+U or the Ease of Access icon (if available)

The available settings have the following meanings are described in the table below:

Feature / Setting	Meaning / Use
Fix mass storage issues	Automatically correct known problems when moving from one mass storage architecture to another. This feature is enabled by default and will resolve most STOP 0x7B errors during Windows guest OS start-up.
Create baseline snapshot	Create a virtual machine snapshot before first launching the VM. You can quickly revert to this snapshot if the VM becomes damaged or you wish to return to the initial guest start-up state without re-creating the VM. This feature is

	enabled by default. Note: This feature is compatible with both VMware Player and VMware Workstation. However, VMware player does not provide a user interface to access the snapshot feature. This is a limitation of VMware Play.er
Logon command prompt (XP only)	Display a system-level (root) command prompt on the login screen. This feature is only available for Windows XP. For later systems, we recommend using the GPR feature (see below) which provides the same feature on all supported Windows operating systems.
Administrator logon on welcome screen (XP only)	This feature is deprecated and will be removed in a future release. We recommend using the GPR feature (see below) which provides the same feature on all supported Windows operating systems.
Split virtual disk into 2GB chunk	Split virtual machine disk files into 2GB chunks. This may be necessary if the files are stored on a file system that does not support large files (e.g. FAT).
Disable auto-reboot on system crash	Prevent Windows guest OS from rebooting if start-up fails. This can be useful to diagnose and troubleshoot start-up problems.
Fix 'known' VM conversion problems	Correct a variety of VM conversion problems caused by problem hardware, drivers, software and OEM utilities. This feature is enabled by default.
Fix XP WPA (XP only)	Temporarily disable Windows XP product activation.
Inject Windows Generic Password Reset (GPR) tool	Install the VFC Generic Password Reset (GPR) tool to Windows guest OS. This tool may be used to reset passwords and gain access to accounts secured with a "live" account.
Limit RAM to 2GB	Limit guest OS RAM to 2GB. The default is to use the RAM size last used (if known). This feature

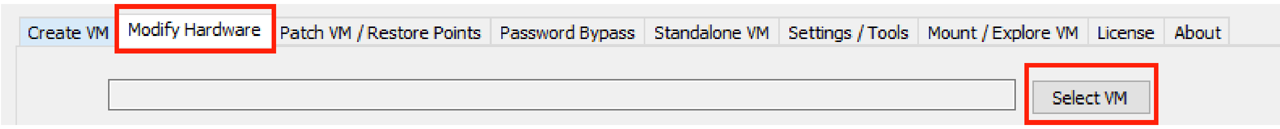
	may be used to work around problems with older operating systems that have issues with large RAM size.
Driver interface	Override the mass storage interface used by VFC. Typically, VFC will automatically select a mass storage interface based on analysis of the guest OS. VFC prefers the SCSI interface but will also use IDE or SATA in certain circumstances. This feature may be used to override the default selection if the guest OS fails to boot. In this case, we recommend selecting the option that matches the original hardware configuration Tip: This may be necessary if VFC is unable to access the guest OS system files. For instance, this can happen if the guest is secured with BitLocker.
OS folder	Override the target OS folder used by VFC. In most cases, VFC will correctly detect the Windows OS folder that contains the system files. However, on some systems with non-standard configuration or dual-boot this may fail. Use this operation to override the default target folder.
Initial display resolution (XP only)	Configure the guest OS display resolution. This feature is only available for Windows XP
Message delay	This feature is no longer used and will be removed from a future release of VFC.
Process delay	This feature is used by Technical Support to workaround problem host system configurations.

Modify Hardware tab (add additional hard drives, network cards etc.)

The **Modify Hardware** tab may be used to conveniently add or remove hardware from the virtual machine configuration directly from within VFC. This may be useful to add additional virtual hard disks or enable networking. A similar feature is directly available in VMware and this may also be used to modify the VM configuration.

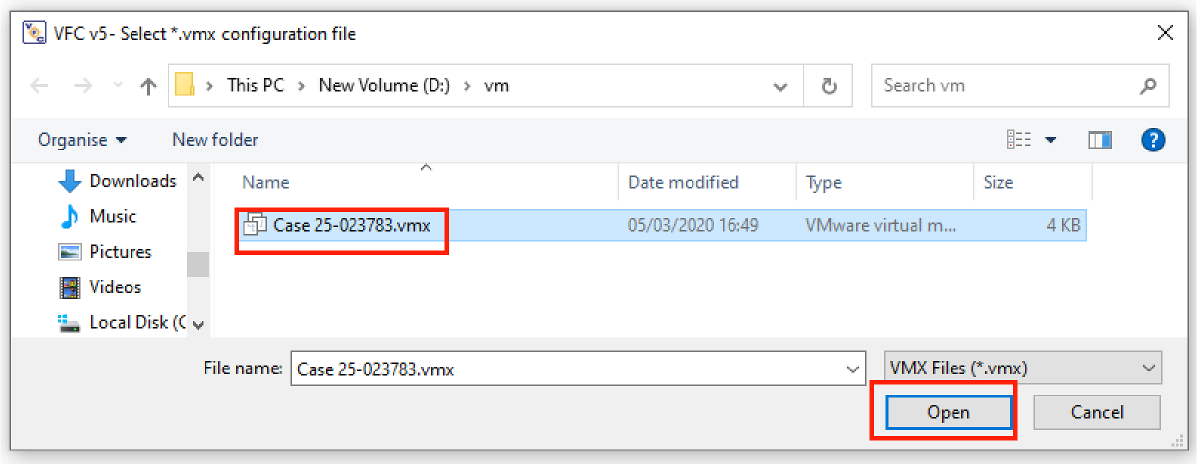
To modify hardware, please proceed as follows:

1. Click **Modify Hardware**



2. Click **Select VM**

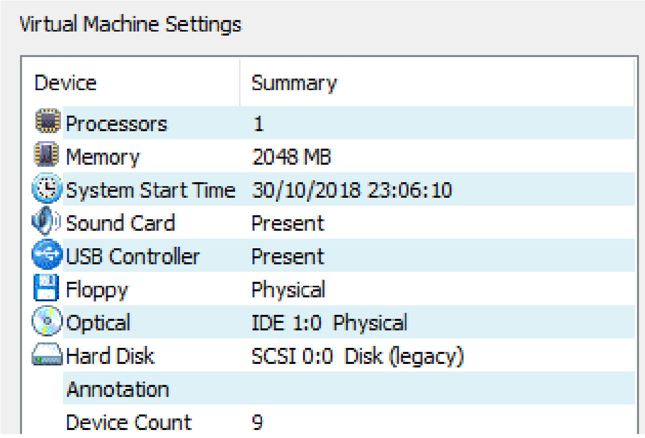
3. Locate the desired virtual machine (VMX file) and click **Open**:



Name	Date modified	Type	Size
Case 25-023783.vmx	05/03/2020 16:49	VMware virtual m...	4 KB

File name: Case 25-023783.vmx

4. Review the virtual hardware configuration:



Virtual Machine Settings

Device	Summary
Processors	1
Memory	2048 MB
System Start Time	30/10/2018 23:06:10
Sound Card	Present
USB Controller	Present
Floppy	Physical
Optical	IDE 1:0 Physical
Hard Disk	SCSI 0:0 Disk (legacy)
Annotation	
Device Count	9

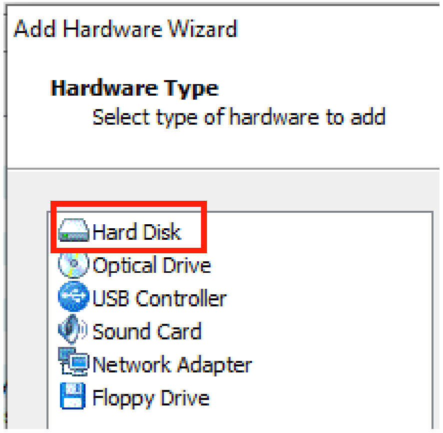
5. If you wish to add hardware, click **Add** and follow the on-screen wizard

6. Similarly, if you wish to remove hardware, click **Remove**

For example, to add a virtual hard disk, proceed as follows:

1. Click **Add**

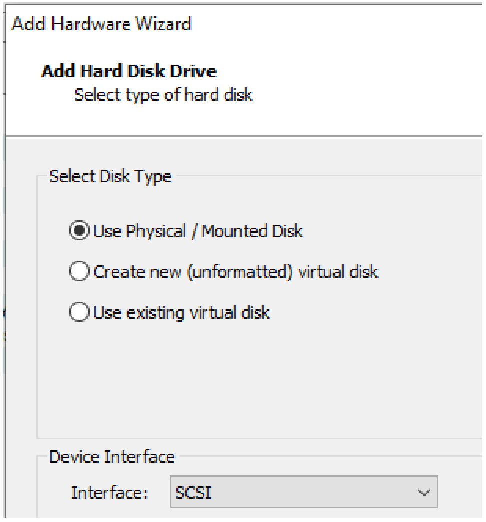
2. Select **Hard Disk** and click **Next**:



Add Hardware Wizard

Hardware Type
Select type of hardware to add

3. Select a disk type and a driver interface:



Add Hardware Wizard

Add Hard Disk Drive
Select type of hard disk

Select Disk Type

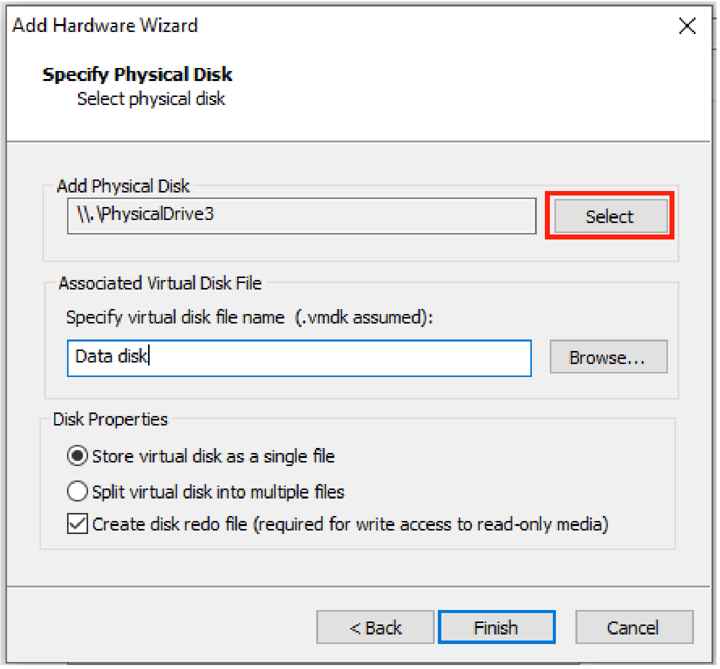
● Use Physical / Mounted Disk
○ Create new (unformatted) virtual disk
○ Use existing virtual disk

Device Interface

Interface: SCSI

TIP: If you wish to add another forensic image, mount that image using VFC Mount (or your preferred mount tool) and then select User Physical / Mounted Disk. The driver interface should normally match that used for the main system disk. In most cases this is SCSI. The exception to this rule is that older (Windows NT 3.x and Windows 9x) systems will typically require IDE and contemporary UEFI-based systems will typically require SATA. If in doubt, try the interface used on the original hardware.

4. Click **Select** and select the desired physical (or emulated) disk, the enter a virtual disk file name and other required disk properties:



Add Hardware Wizard

Specify Physical Disk
Select physical disk

Add Physical Disk
\\.\PhysicalDrive3

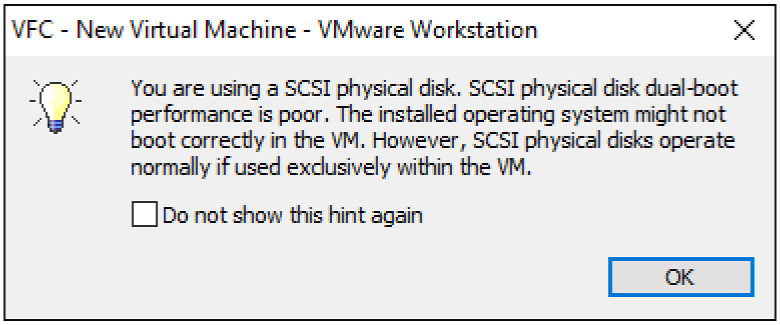
Associated Virtual Disk File
Specify virtual disk file name (.vmdk assumed):
Data disk

Disk Properties
● Store virtual disk as a single file
○ Split virtual disk into multiple files
☑ Create disk redo file (required for write access to read-only media)

5. Click **Finish** and then **Save** to complete the process

VMware SCSI warning

When starting the VM for the first time, you may see the following message:



VFC - New Virtual Machine - VMware Workstation

You are using a SCSI physical disk. SCSI physical disk dual-boot performance is poor. The installed operating system might not boot correctly in the VM. However, SCSI physical disks operate normally if used exclusively within the VM.

□ Do not show this hint again

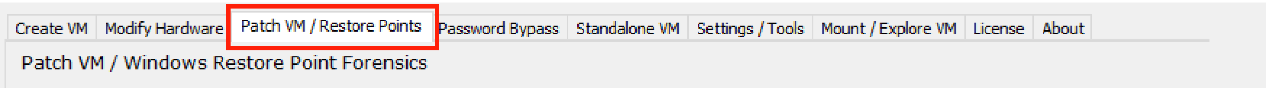
This message indicates that VMware may perform better with a non-SCSI mass storage interface. However, VFC prefers the SCSI interface because, whilst it may have marginally poorer performance it is more likely to result in a successful VM conversion. In most cases, you can safely tick the box and ignore this warning.

Patch VM / Restore Points tab (VM repair)

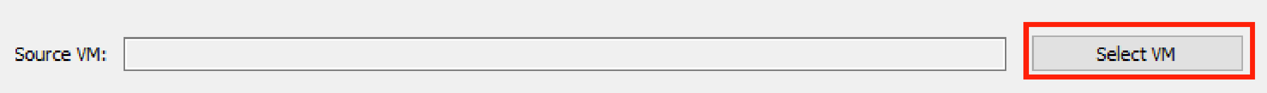
The **Patch VM / Restore Points** tab may be used to repair an existing VM that fails to boot or is otherwise not functional. This re-applies the various compatibility changes provided by VFC and is similar to the process used when creating a new VM. This procedure can be particularly useful after using the Windows System Restore feature to restore the guest system to a previous point. This may remove the changes made by VFC and leave the system in an unusable state.

To patch a VM, please proceed as follows:

1. Click **Patch VM / Restore Points**:

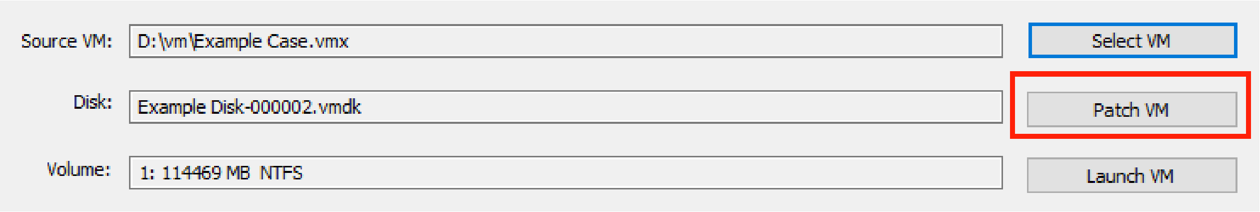


2. Click **Select VM**, locate the desired virtual machine (VMX file) and then click **Open**:



3. If prompted, select the target system partition (this is only necessary if multiple partitions are present)

4. Click **Patch VM** and wait for the operation to complete (this will typically take a few seconds):



Source VM: D:\vm\Example Case.vmx

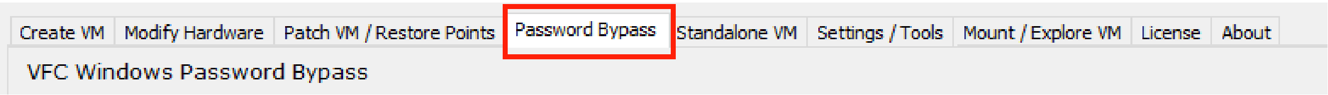
Disk: Example Disk-000002.vmdk

Volume: 1: 114469 MB NTFS

5. Click **Launch VM** to start the virtual machine and confirm that it is now functional

Password Bypass tab (PWB)

The **Password Bypass** tab may be used to gain access to password protected Windows systems. The PWB operates by performing an in-memory patch on the guest OS to temporarily disable password authentication. This is useful to gain temporary access and the normal configuration is restored when the VM is next restarted:



VFC Windows Password Bypass

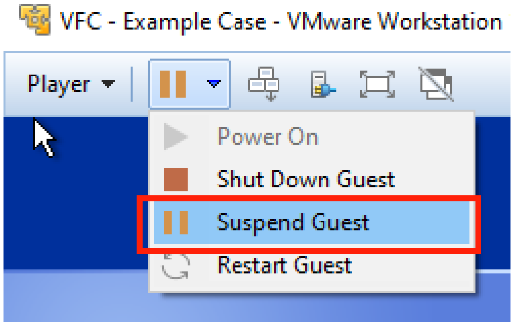
TIP: The PWB feature can be very useful but does not support Windows "live" accounts. To access these accounts, a system-level (root) command prompt and make persist password changes please use the Generic Password Reset (GPR) feature. This is described later in this guide. Please note that PWB is currently only available for Windows guest OS.

To use the PWB feature, please proceed as follows:

1. Start the Windows-based VM and wait for it to boot to the login prompt

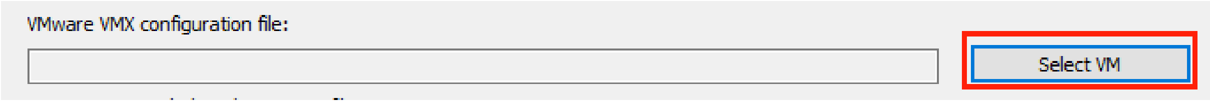
2. Attempt to log in with any password (this will fail)

3. Use VMware to suspend (pause) the virtual machine:



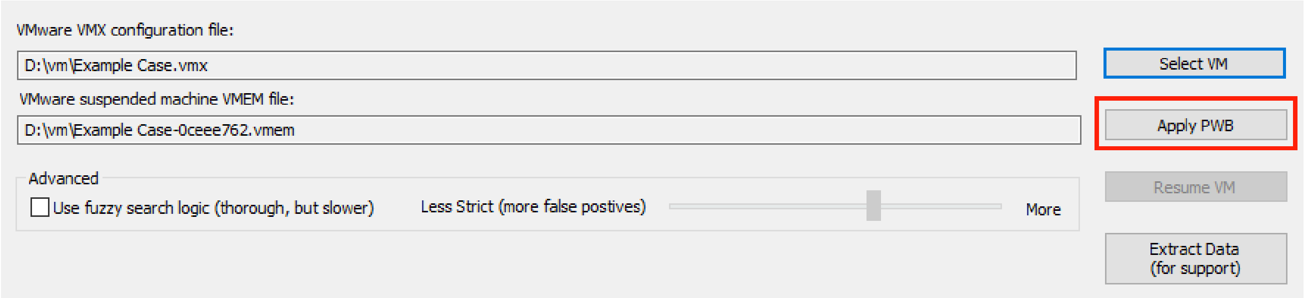
4. Open VFC and click **Password Bypass**

5. Click **Select VM**, locate the desired virtual machine (VMX file) and then click **Open**:



6. If prompted, select the target system partition (this is only necessary if multiple partitions are present)

7. Click **Apply PWB** to patch the virtual machine:



VMware VMX configuration file: D:\vm\Example Case.vmx

VMware suspended machine VMEM file: D:\vm\Example Case-0ceee762.vmem

Advanced

☐ Use fuzzy search logic (thorough, but slower)

TIP: The message "No associated memory file (.vmem) present" indicates the VM is not in a suspended start. Please launch the VM, wait for it to boot and suspend it using VMware before trying again.*

8. If the process is successful, click **Resume VM**

9. Attempt to login to any local account using any password

TIP: This process cannot be used for Windows "live" accounts. Please use the GPR feature to access such accounts. This is described later in this guide.

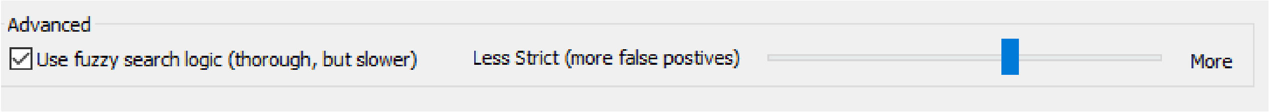
Troubleshooting PWB

In some cases, VFC PWB may not be successful. For instance, this can happen if the guest Windows edition/revision has not been encountered before. In this case, the “fuzzy logic” feature may be used to speculatively apply a PWB patch. This may not work in all cases but may be successful if the Windows edition is similar to a previous version.

To use “fuzzy logic”, please proceed as follows:

1. Setup PWB as described above but do not click **Apply PWB**

2. Tick the “Use fuzzy search logic” checkbox



Advanced

☑ Use fuzzy search logic (thorough, but slower)

Less Strict (more false postives)

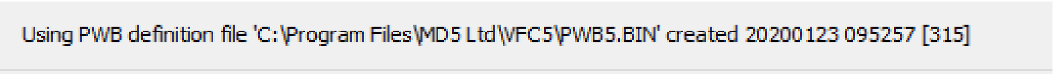
3. Click **Apply PWB**

TIP: In some cases, fuzzy logic may fail or produce false positives that lead to an unusable virtual machine. In this case, try adjusting the slider to make the process more or less strict. Less strict will result in more false positives and may increase the chances of producing an unviable VM.

In some cases, PWB may fail even with the “fuzzy logic” option enabled. In this situation, we would suggest you try the following:

1. Check that you are using the latest PWB definition file:

   a. The current PWB file is shown at the bottom of the PWB tab:



Using PWB definition file 'C:\Program Files\MD5 Ltd\VFC5\PWB5.BIN' created 20200123 095257 [315]

   b. Please visit the VFC website and check if a newer PWB file is available
   c. Please see the VFC FAQ for PWB definition installation instructions

2. Try the Generic Password Reset (GPR) feature. This supports a wider range of scenarios than the original VFC PWB feature including “live” accounts

3. Use the password hashes to crack the original password

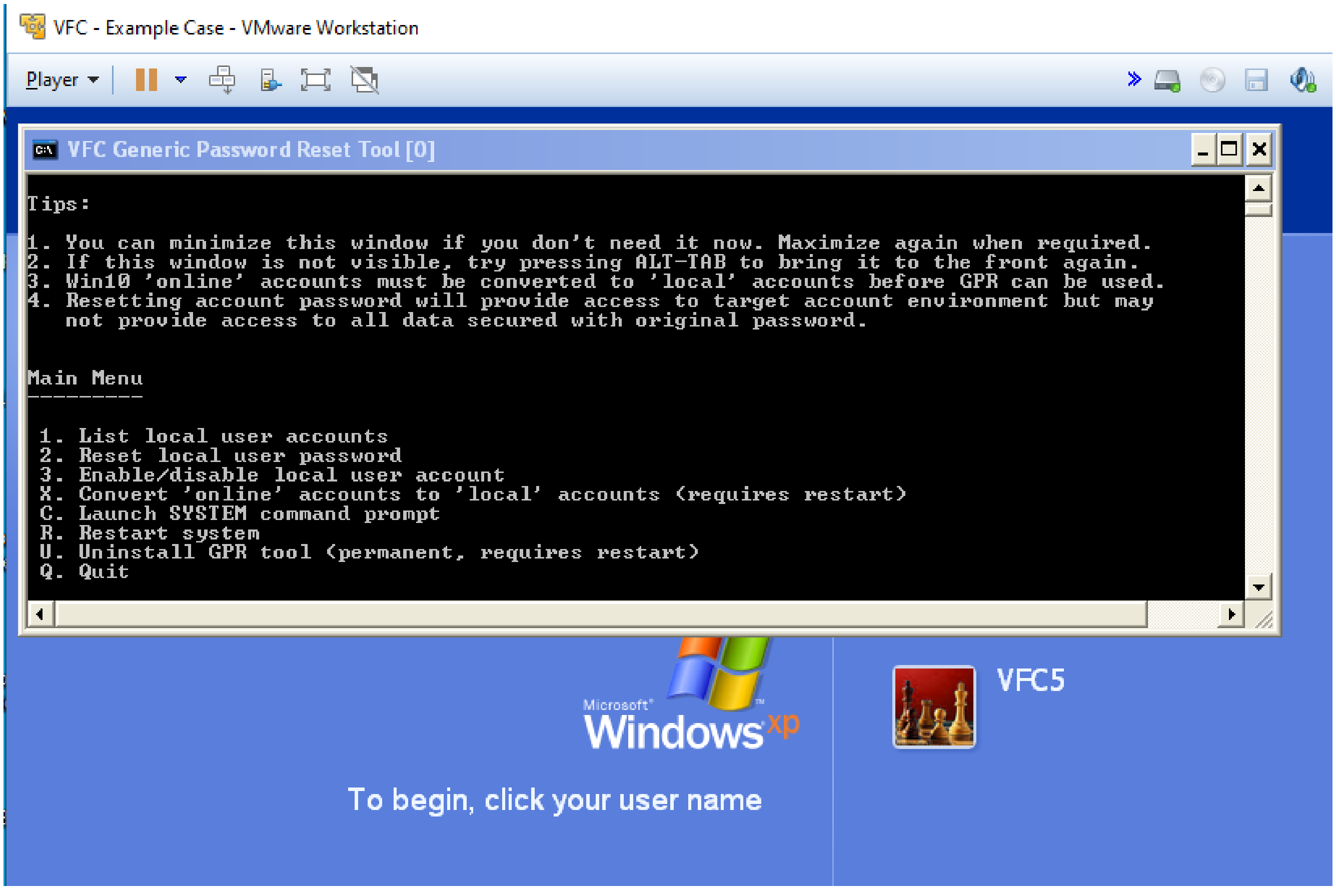
4. Send VFC Technical Support a copy of relevant Windows system files from the guest OS. This does not include any confidential or case-specific data. To do this: Click **Extract Data** and follow the on-screen instructions to generate a VFC5.PWB file

Generic Password Reset feature (GPR) for Live ID account access

The Generic Password Reset (GPR) feature provides a powerful alternative to the original VFC PWB feature. It uses a completely different technique that can be used to make permanent account and password changes:

- Change Windows online “live” user accounts to “local” user accounts
- Reset password for local accounts to a known value
- Launch a Command Prompt with system-level privileges

GPR operates by injecting a VFC software component directly into a Windows-based virtual machine. This feature is enabled by default and may be disabled using the VFC Options dialog. GPR displays a console (text) application on the login screen which can be used to list and manipulate user accounts and launch a system (root) command-prompt.


VFC - Example Case - VMware Workstation
Player
VFC Generic Password Reset Tool [0]
Microsoft Windows xp
To begin, click your user name
VFC5

```
Tips:

1. You can minimize this window if you don't need it now. Maximize again when required.
2. If this window is not visible, try pressing ALT-TAB to bring it to the front again.
3. Win10 'online' accounts must be converted to 'local' accounts before GPR can be used.
4. Resetting account password will provide access to target account environment but may
   not provide access to all data secured with original password.


Main Menu
---------

 1. List local user accounts
 2. Reset local user password
 3. Enable/disable local user account
 X. Convert 'online' accounts to 'local' accounts (requires restart)
 C. Launch SYSTEM command prompt
 R. Restart system
 U. Uninstall GPR tool (permanent, requires restart)
 Q. Quit
```

The GPR tool usually starts within a few seconds of the logon desktop being displayed and emits a beep sound as it starts. If the tool is not visible, please try one of the following techniques:

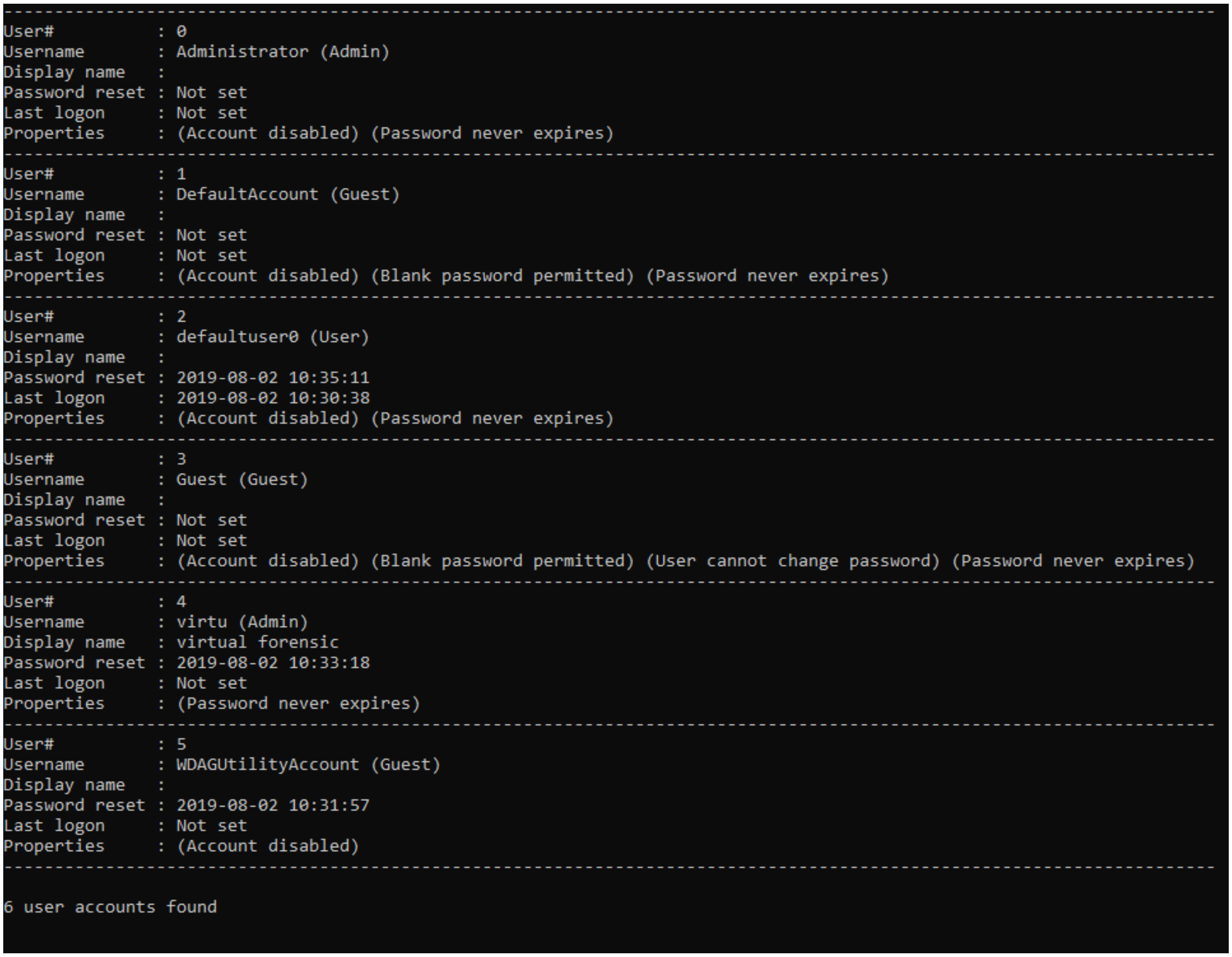
a. Press Alt-Tab to cycle trough available applications
b. Press shift five times (Windows XP)
c. Click the Windows Ease of Access icon (Windows Vista and later)

TIP: If the GPR tool is still not visible, please see the VFC FAQ for troubleshooting tips.

To use the GPR feature, please select an option from the menu and follow the on-screen instructions.

Listing local accounts

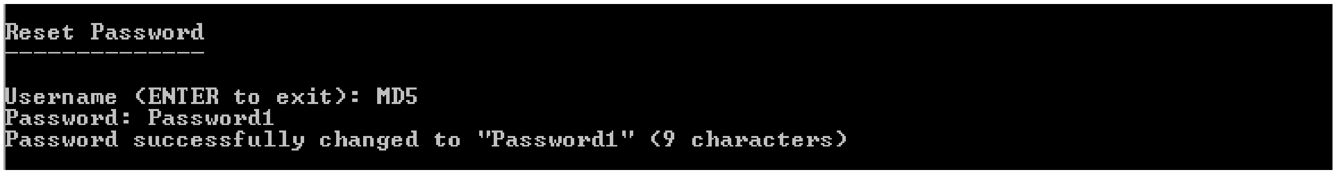
To list local accounts with GPR, press **1** and note the **Username** (not display name) field of the desired account:



```
-----------------------------------------------------------------------------------------------------------------------
User#          : 0
Username       : Administrator (Admin)
Display name   :
Password reset : Not set
Last logon     : Not set
Properties     : (Account disabled) (Password never expires)
-----------------------------------------------------------------------------------------------------------------------
User#          : 1
Username       : DefaultAccount (Guest)
Display name   :
Password reset : Not set
Last logon     : Not set
Properties     : (Account disabled) (Blank password permitted) (Password never expires)
-----------------------------------------------------------------------------------------------------------------------
User#          : 2
Username       : defaultuser0 (User)
Display name   :
Password reset : 2019-08-02 10:35:11
Last logon     : 2019-08-02 10:30:38
Properties     : (Account disabled) (Password never expires)
-----------------------------------------------------------------------------------------------------------------------
User#          : 3
Username       : Guest (Guest)
Display name   :
Password reset : Not set
Last logon     : Not set
Properties     : (Account disabled) (Blank password permitted) (User cannot change password) (Password never expires)
-----------------------------------------------------------------------------------------------------------------------
User#          : 4
Username       : virtu (Admin)
Display name   : virtual forensic
Password reset : 2019-08-02 10:33:18
Last logon     : Not set
Properties     : (Password never expires)
-----------------------------------------------------------------------------------------------------------------------
User#          : 5
Username       : WDAGUtilityAccount (Guest)
Display name   :
Password reset : 2019-08-02 10:31:57
Last logon     : Not set
Properties     : (Account disabled)
-----------------------------------------------------------------------------------------------------------------------

6 user accounts found
```

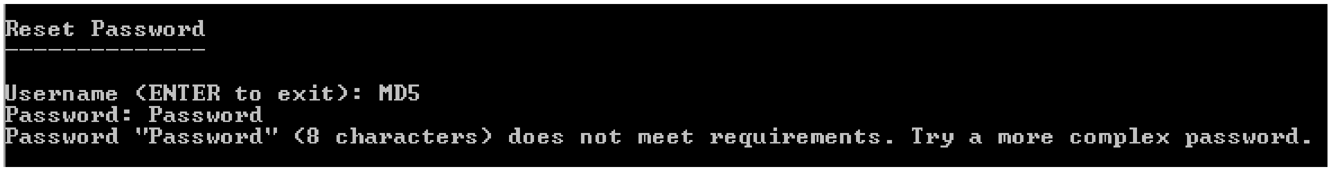
Change local account password to a known value

To change a local account password with GPR, press **2** and enter the **Username** (not the display name) and then a new password:

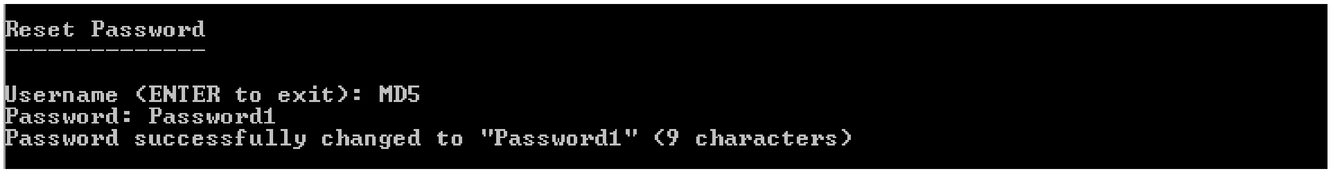


```
Reset Password
--------------

Username (ENTER to exit): MD5
Password: Password1
Password successfully changed to "Password1" (9 characters)
```

In some cases, the new password may not need the password complexity rules of the guest system. In this case, try again with a longer and more complex password (e.g. alphanumeric or with a mix of cases or including some symbols). For example:



```
Reset Password
--------------

Username (ENTER to exit): MD5
Password: Password
Password "Password" (8 characters) does not meet requirements. Try a more complex password.
```

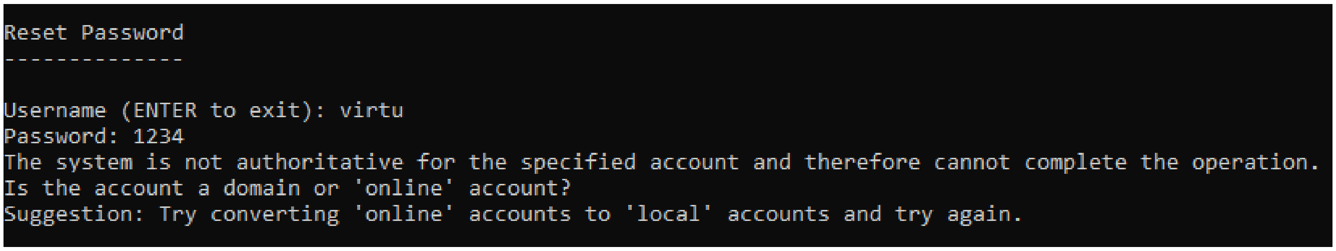


```
Reset Password
--------------

Username (ENTER to exit): MD5
Password: Password1
Password successfully changed to "Password1" (9 characters)
```

TIP: Depending on the security policy settings, you may need to enhance the security of your replacement password before the guest OS will accept it.

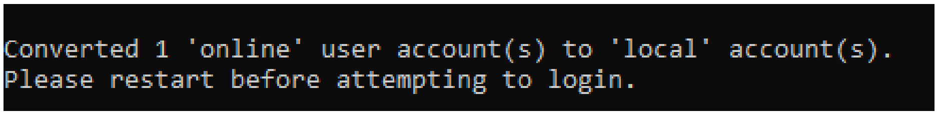
Change “live” account to local account

In some cases, GPR may report that “The system is not authoritative for the specified account”. This typically indicates that the account is a “live” account and cannot be reset using the standard technique:



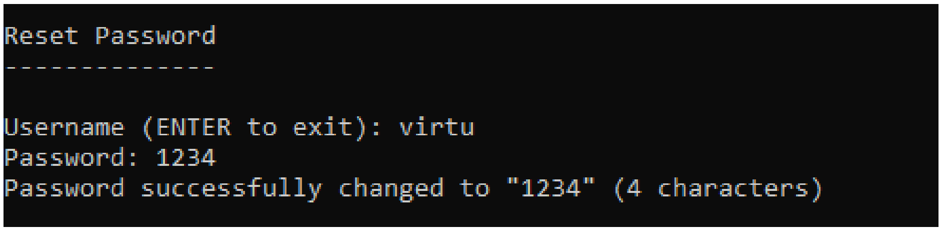
```
Reset Password
--------------

Username (ENTER to exit): virtu
Password: 1234
The system is not authoritative for the specified account and therefore cannot complete the operation.
Is the account a domain or 'online' account?
Suggestion: Try converting 'online' accounts to 'local' accounts and try again.
```

In this case, press X to convert the “live” (online) account to a local account and then press R to restart the guest OS:



```
Converted 1 'online' user account(s) to 'local' account(s).
Please restart before attempting to login.
```

When the system has restarted, press **2** to repeat the previous procedure and reset the newly converted local account password:



```
Reset Password
--------------

Username (ENTER to exit): virtu
Password: 1234
Password successfully changed to "1234" (4 characters)
```

GPR tips and tricks

The GPR feature is very powerful and loads each time the VM starts. The following GPR features may also be useful:

- Menu C – Launches a system-level (root) command prompt. This can be used for a variety of tasks including running third-party tools, creating additional user accounts or extracting/cracking the SAM (user accounts) registry key

- Menu U – Uninstalls the GPR tool so that it no longer launches at start-up. We recommend using this option before creating a standalone clone VM

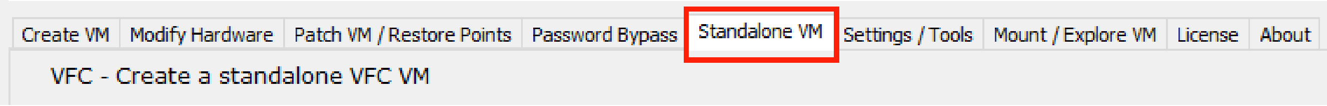
- Menu R – Restarts the guest system. This is necessary after converting “live” accounts to local accounts

- Menu Q – Quits the GPR tool for the current session. The tool will be available again after the VM has been restarted. Alternatively, you can minimise the GPR window and restore it using the Alt-Tab keys.

Please note, neither PWB nor GPR currently support bypass of domain authenticated passwords. This is a focus of on-going research and we hope to provide a solution in the future.

Standalone VM tab

The **Standalone VM** tab may be used to copy an existing VFC virtual machine into a standalone VM that is independent of VFC. This may be useful if you wish the VM to be used by other team members or exhibited in court or similar. The new VM is free-standing and does not require the original image files, VFC Mount or other mount tools.



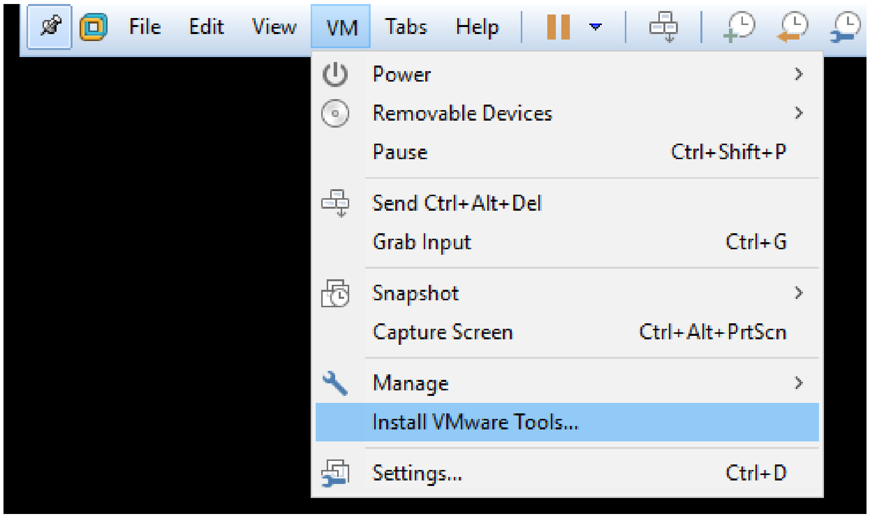
TIP: A standalone VM may take some time to generate and, once created, will no longer have access to the features of VFC. We recommend that you configure the VM fully using VFC before using this feature. Typically, this may mean resetting account password using PWB or GPR, updating drivers and installing VM Tools.

TIP: Please remember that a standalone VM is a copy of the original VM at a point in time. Subsequent changes to the standalone copy will be retained in the copy and it will no longer be a (forensic) copy of the original material.

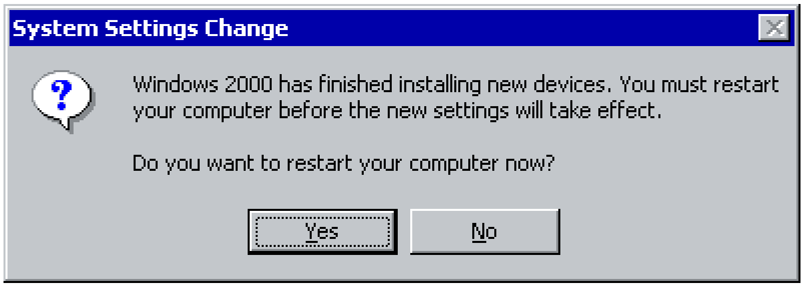
Preparation for standalone clone VM

Before creating a VM Standalone Clone, we recommend that you complete the following:

1. Install VMware Tools



2. Reboot the VM and resolve any outstanding missing drivers. Repeat this process until the VM starts cleanly as does not display a message similar to this:



System Settings Change

Windows 2000 has finished installing new devices. You must restart your computer before the new settings will take effect.

Do you want to restart your computer now?

3. Reset passwords to known values. This can be achieved using one of the following techniques:

    a. Use the VFC GPR tool to convert Windows “live” accounts to “local” accounts and permanently change passwords

       Or

    b. Use the VFC PWB feature to attain temporary system access and then change passwords using the built-in Windows tools

4. Cleanly shutdown the VM

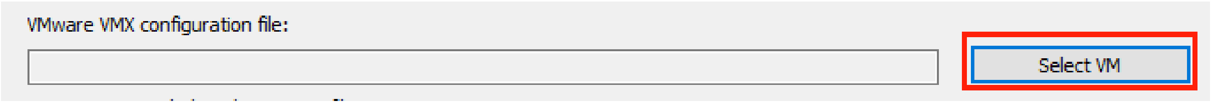
TIP: You must shut down the VM in VMware before you can use the Standalone VM feature

Creating the standalone clone VM

Once the procedures above have been performed, please proceed as follows to create a standalone VM:

1. Open VFC and click **Standalone VM**

2. Click **Select VM**, locate the desired virtual machine (VMX file) and then click **Open**:



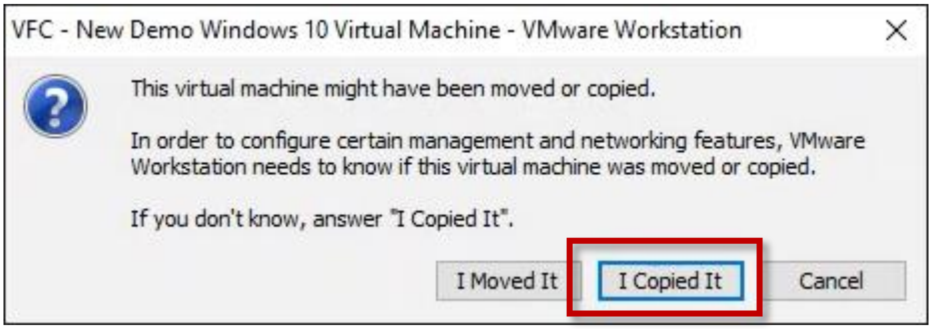
3. Click **Select Target** and choose a location for the target virtual machine (VMX file)

4. Click **Export Clone**

Launching the standalone clone VM

Following the creation of the standalone clone VM, you can copy the new VM to another folder or backup medium and then launch it independently using VMWare Player / Workstation.

In some cases, the following message may be displayed when the VM is first started. Please click **I Copied It** to continue:



VFC - New Demo Windows 10 Virtual Machine - VMware Workstation

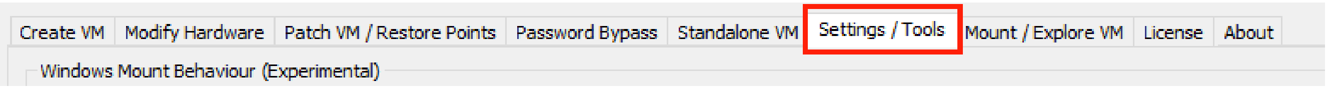
This virtual machine might have been moved or copied.

In order to configure certain management and networking features, VMware Workstation needs to know if this virtual machine was moved or copied.

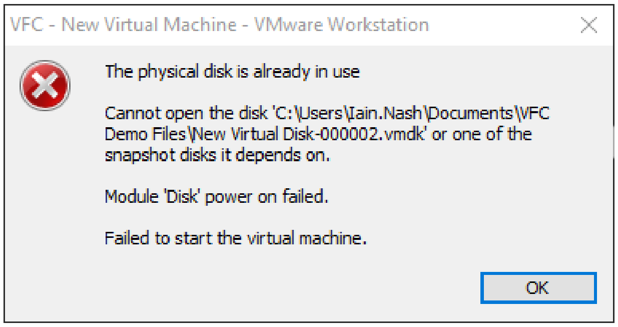
If you don't know, answer "I Copied It".

Settings / Tools tab

The **Settings / Tools** tab may be used to configure the host system for use with VFC and VMware. The principal use of this tab is to modify the host system mount behaviour to avoid the notorious "Physical Disk In Use" (PDIU) error in VMware:



This error occurs because the host Windows system can attempt to mount the emulated physical disk used by VFC/VMware and then lock it. This prevents VMware from acquiring exclusive access to the disk and leads to the VMware error message "Physical drive already in use":



VFC - New Virtual Machine - VMware Workstation

The physical disk is already in use

Cannot open the disk 'C:\Users\Iain.Nash\Documents\VFC Demo Files\New Virtual Disk-000002.vmdk' or one of the snapshot disks it depends on.

Module 'Disk' power on failed.

Failed to start the virtual machine.

TIP: We recommend using VFC Mount as the preferred mount tool because it contains features which have been specifically designed to minimise this problem and improve compatibility with VMware. This feature may not be available in third-party mount tools.

To resolve this problem please proceed as follows:

1. Unmount any existing images, close your mount tool and close VFC

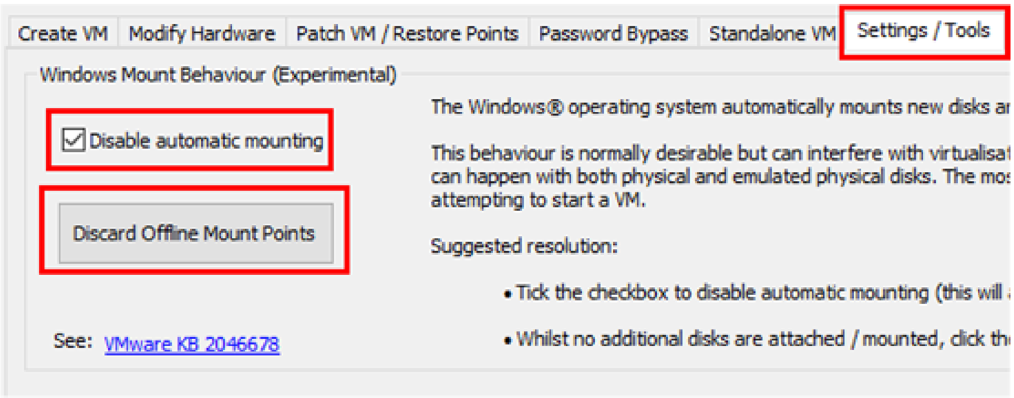
   NB: You can quit VFC Mount by right-clicking on the notification area icon and selecting "Exit". Alternatively, reboot your machine.

2. Re-start VFC and navigate to the **Settings/Tools** tab

3. Tick the **Disable automatic mounting** checkbox. This disables the default Windows behaviour.

   NB: It will also mean that future drives mounted on your system are not automatically assigned drive letters. You can assign them manually via the Windows Disk Manager tool

4. Click the **Discard Offline Mount Points** button and follow the on-screen instructions. This discards the Windows history of previously mounted disk/drive letter assignments. It ensures that any images previously mounted on the system are forgotten and will not auto-mount again in the future.



Windows Mount Behaviour (Experimental)

☑ Disable automatic mounting

The Windows® operating system automatically mounts new disks ar

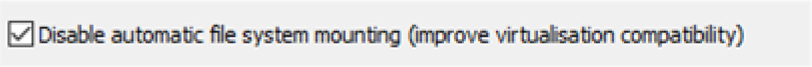
This behaviour is normally desirable but can interfere with virtualisat
can happen with both physical and emulated physical disks. The mos
attempting to start a VM.

Suggested resolution:

- Tick the checkbox to disable automatic mounting (this will
- Whilst no additional disks are attached / mounted, click th

See: VMware KB 2046678

5. Start **VFC Mount**. This has the same checkbox and it should already be ticked:

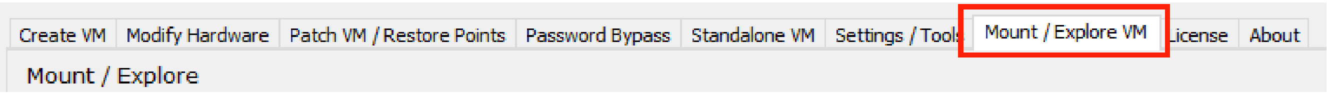


☑ Disable automatic file system mounting (improve virtualisation compatibility)

TIP: Occasionally, Windows can lock a disk and refuse to release it. If this happens (including with VFC Mount) try rebooting the host system. This will resolve the problem in most cases. The following article from VMware provides more technical information on the issue: *https://kb.vmware.com/s/article/2046678*

Mount / Explore VM tab

The **Mount / Explore VM** tab may be used to mount an existing virtual machine disk and manipulate the file system that it contains. This can be used to conveniently transfer files both to and from the VM and make other configuration changes before starting the virtual machine:



The feature is very powerful but could also inadvertently expose the host (examination) system to files and programs within the guest VM environment. For this reason, we recommend that the feature is used cautiously and only after assessing the risks involved. The feature currently has the following requirements and limitations:

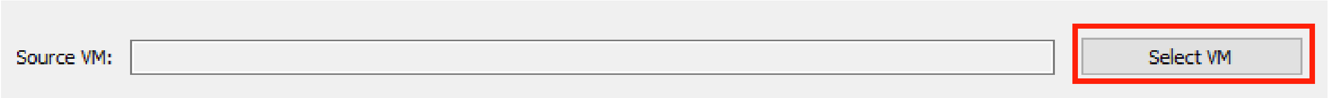
- The VM must be in a shutdown state (not running or suspended)
- The VM must be unmounted before attempting to use other VFC features or VMware
- Only Windows-compatible file systems (FAT and NTFS) are currently supported
- Copy / Paste outside of VFC is limited because VFC runs as an elevated (administrator) process and Windows Explorer typically does not. To avoid problems, we recommend only using the user interface within VFC for copy/paste.

- GPT partitions are not currently supported

To explore a VM file system, please proceed as follows:

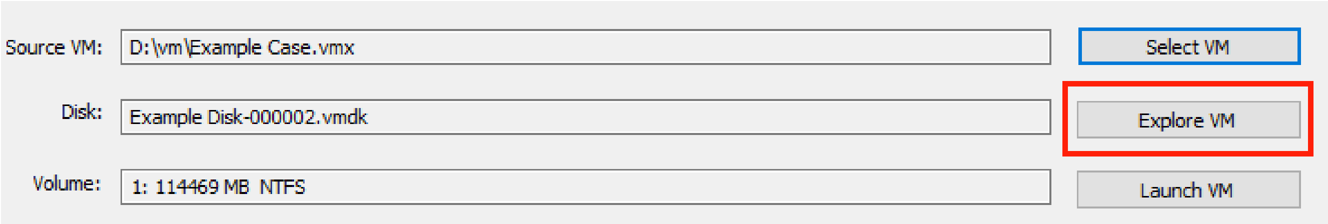
1. Click the **Mount / Explore VM tab**

2. Click **Select VM**, locate the desired virtual machine (VMX file) and then click **Open**:



3. If prompted, select the target system partition (this is only necessary if multiple partitions are present)

4. Click **Explore VM** and wait for the mount operation to complete (this will typically take a few seconds):

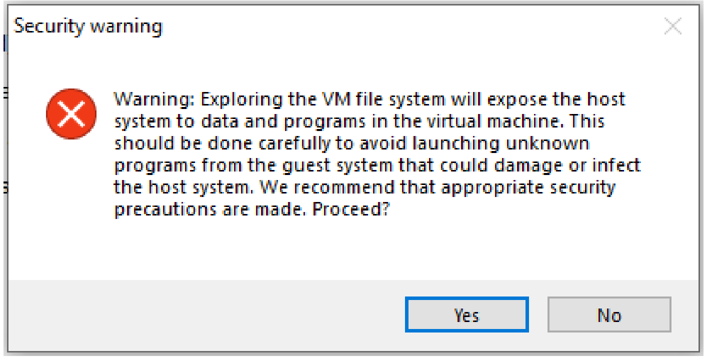


Source VM: D:\vm\Example Case.vmx

Disk: Example Disk-000002.vmdk

Volume: 1: 114469 MB NTFS

5. Read the security warning and, if you wish to continue, click **Yes:**

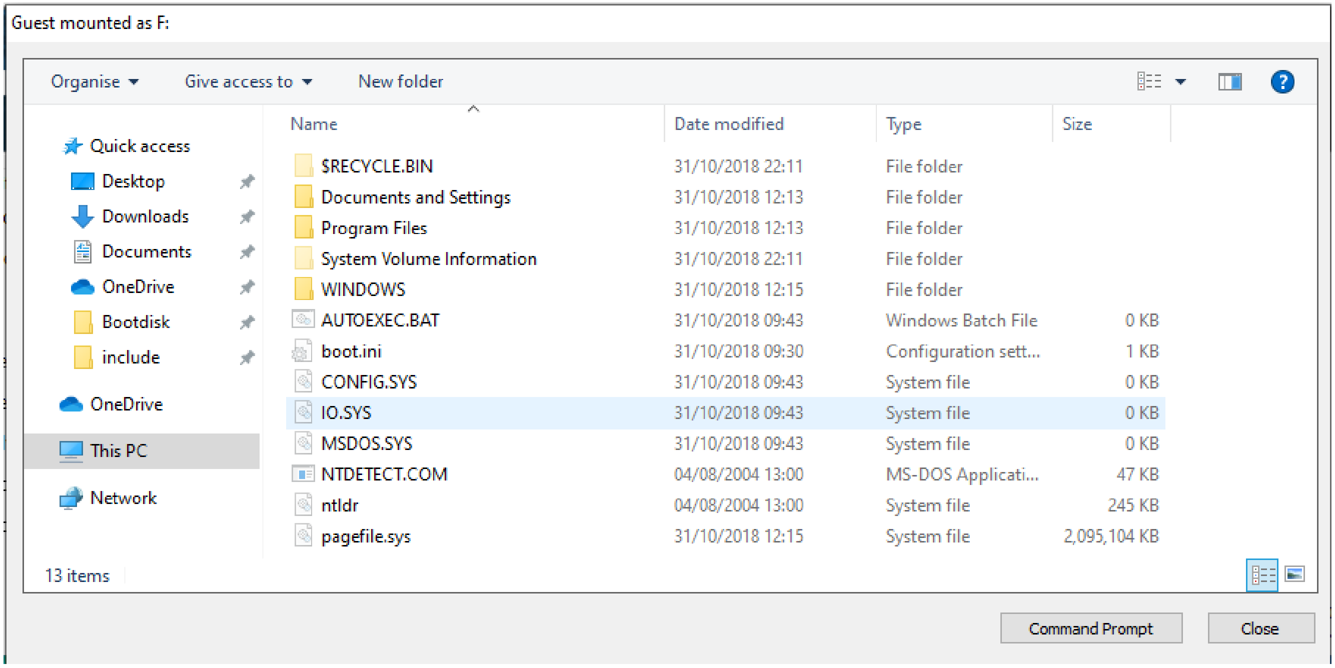


Security warning

Warning: Exploring the VM file system will expose the host system to data and programs in the virtual machine. This should be done carefully to avoid launching unknown programs from the guest system that could damage or infect the host system. We recommend that appropriate security precautions are made. Proceed?

6. Use the file system dialog to copy/paste files and make any required system changes

TIP: We recommend confining file operations to within the dialog. Do not try to copy/paste from the dialog to Windows Explorer or vice versa. This will typically fail unless Windows Explorer is also running as an elevated process.



Guest mounted as F:

Name	Date modified	Type	Size
$RECYCLE.BIN	31/10/2018 22:11	File folder	
Documents and Settings	31/10/2018 12:13	File folder	
Program Files	31/10/2018 12:13	File folder	
System Volume Information	31/10/2018 22:11	File folder	
WINDOWS	31/10/2018 12:15	File folder	
AUTOEXEC.BAT	31/10/2018 09:43	Windows Batch File	0 KB
boot.ini	31/10/2018 09:30	Configuration sett...	1 KB
CONFIG.SYS	31/10/2018 09:43	System file	0 KB
IO.SYS	31/10/2018 09:43	System file	0 KB
MSDOS.SYS	31/10/2018 09:43	System file	0 KB
NTDETECT.COM	04/08/2004 13:00	MS-DOS Applicati...	47 KB
ntldr	04/08/2004 13:00	System file	245 KB
pagefile.sys	31/10/2018 12:15	System file	2,095,104 KB

13 items

7. If necessary, click **Command Prompt** to open a command prompt on the target file system. This may be useful to perform more complex modifications.

   TIP: Please remember to close the command prompt when finished and before attempting to unmount the VM.

8. When finished, click **Close** to unmount the VM

Experiencing the original user's Desktop

Following the successful creation of a virtual machine and bypass of user passwords, you should be able to login to the desired user account and experience the user's original desktop environment.

Depending on the original hardware and the number of changes made by VFC, it is quite likely that you will experience several operating system prompts to install new hardware and sometimes to reboot. If the VM is stable, and you only intend to access it briefly, you can usually safely ignore these prompts. However, if the VM is not fully usable or you intend to use the system for a prolonged period or to create a standalone VM, we recommend that you install VMware Tools, complete any outstanding driver installation and if prompted, reboot. This will typically result in a more stable and usable virtual machine experience.

Installation of VMware Tools can resolve problems such:

- Incorrect screen resolution / colour display
- Jumpy mouse
- Poor VM performance

You may also like to manually modify the following:

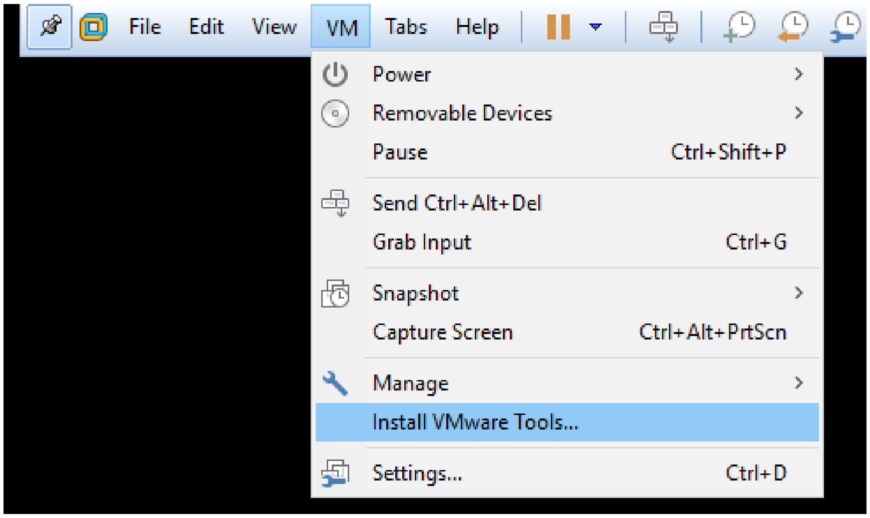
- Screen resolution
- Enable/disable sound
- Enable networking (with caution)

Please see the section below for tips on installing VMware Tools.

VMware Tools Installation

In most instances, we recommend the installation of VMware Tools. This will typically take a minute or two. To install, please proceed as follows:

1. Click the **VM/ Install VMware Tools** (other methods are also available):



2. Follow the on-screen prompts

3. If prompted, **Restart** the guest OS

TIP: Installing VMware Tools will typically generate a Windows System Restore checkpoint. This may lead to the deletion of a previous checkpoint and associated data. If this may be relevant to the specific case, we would suggest that you avoid installing VMWare Tools.

*TIP: Use of Windows System Restore to a previous point-in-time will also uninstall VMWare Tools and may lead to an unbootable VM. In this case, use the **Patch VM/ Restore Point** tab to fix the VM and then install VMware Tools again if necessary. An example of this scenario is given below.*

Detailed information on VMware Tools is available in the VMware Workstation User's Manual:

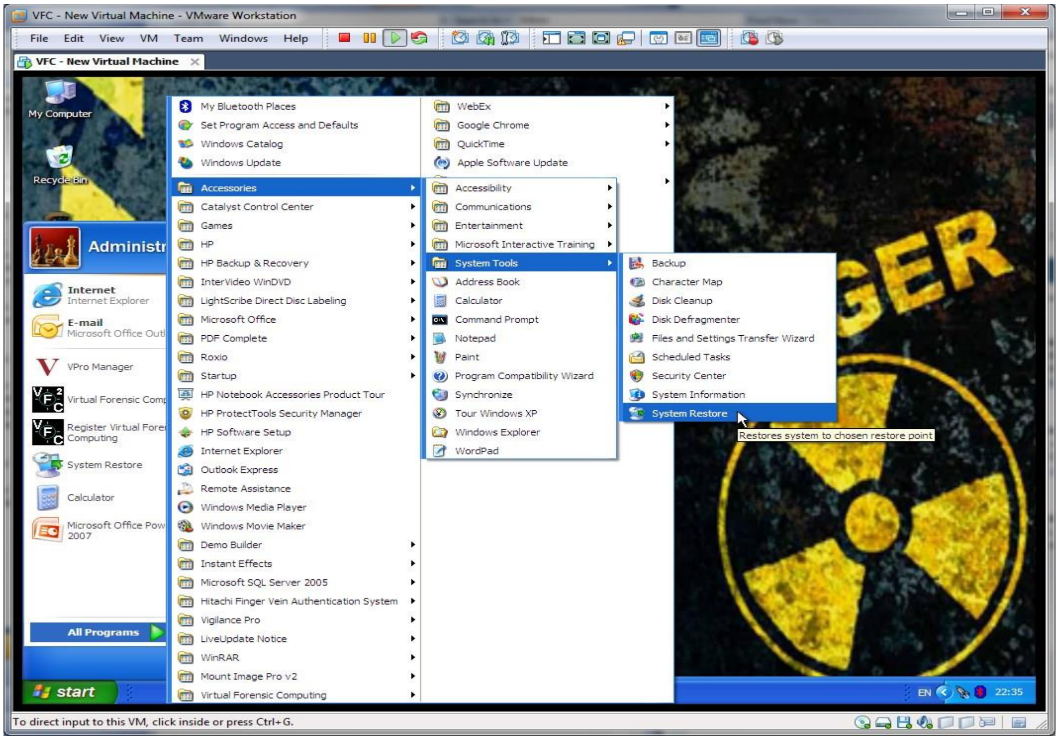
https://docs.vmware.com/en/VMware-Workstation-Pro/15.0/workstation-pro-15-user-guide.pdf

Example: Using Windows System Restore and VFC Patch VM / Restore Points tab

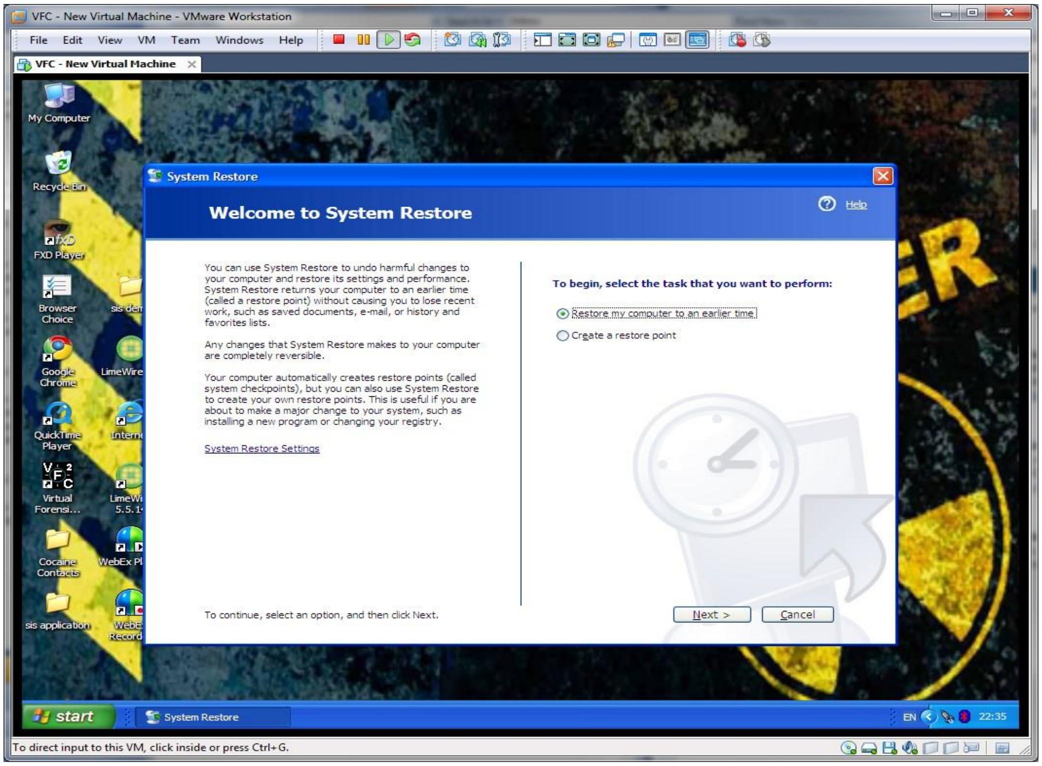
It may be desirable to use the Windows System Restore feature to “rewind” a VM to a previous point-in-time. In many cases, this will lead to the VM becoming unbootable because the system restore process will also remove the compatibility changes made by VFC. The following section explains how to use System Restore and then the VFC Patch VM / Restore Points tab to repair the VM so that it be used within VMware again.

The following example is for Windows XP. A similar process may be used for later operating system:

1. Launch the **Windows System Restore** utility:



2. Follow the on-screen prompts to select a restore point and then wait for the restore process to complete (this may take some time):



VFC - New Virtual Machine - VMware Workstation

System Restore

Welcome to System Restore

Help

You can use System Restore to undo harmful changes to your computer and restore its settings and performance. System Restore returns your computer to an earlier time (called a restore point) without causing you to lose recent work, such as saved documents, e-mail, or history and favorites lists.

Any changes that System Restore makes to your computer are completely reversible.

Your computer automatically creates restore points (called system checkpoints), but you can also use System Restore to create your own restore points. This is useful if you are about to make a major change to your system, such as installing a new program or changing your registry.

System Restore Settings

To begin, select the task that you want to perform:

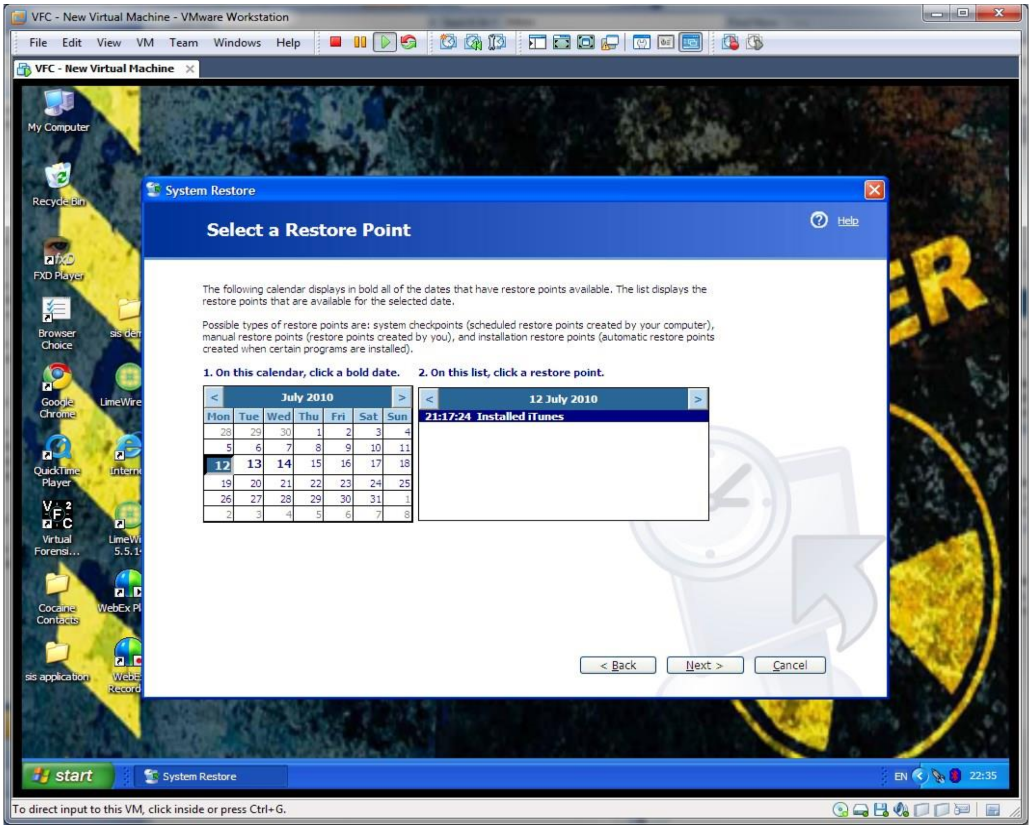
● Restore my computer to an earlier time

○ Create a restore point

To continue, select an option, and then click Next.

Next > Cancel

To direct input to this VM, click inside or press Ctrl+G.



VFC - New Virtual Machine - VMware Workstation

System Restore

Select a Restore Point

Help

The following calendar displays in bold all of the dates that have restore points available. The list displays the restore points that are available for the selected date.

Possible types of restore points are: system checkpoints (scheduled restore points created by your computer), manual restore points (restore points created by you), and installation restore points (automatic restore points created when certain programs are installed).

1. On this calendar, click a bold date.

July 2010

Mon	Tue	Wed	Thu	Fri	Sat	Sun
28	29	30	1	2	3	4
5	6	7	8	9	10	11
12	**13**	**14**	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	1
2	3	4	5	6	7	8

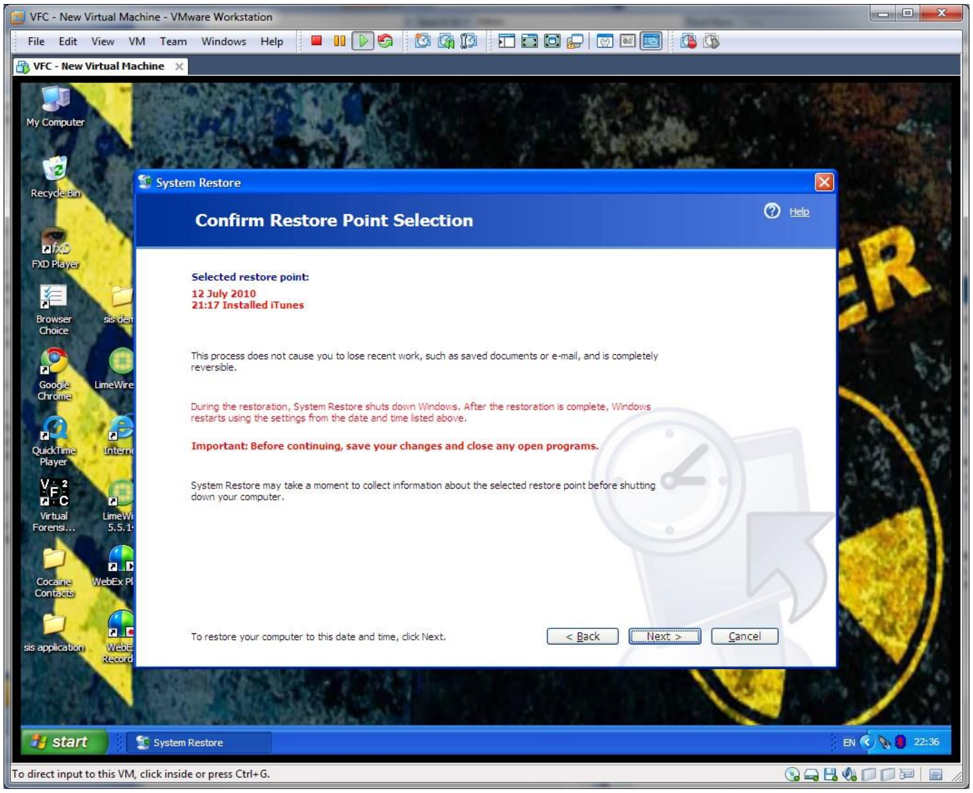
2. On this list, click a restore point.

12 July 2010

21:17:24 Installed iTunes

< Back Next > Cancel

To direct input to this VM, click inside or press Ctrl+G.



System Restore

Confirm Restore Point Selection

Help

Selected restore point:
12 July 2010
21:17 Installed iTunes

This process does not cause you to lose recent work, such as saved documents or e-mail, and is completely reversible.

During the restoration, System Restore shuts down Windows. After the restoration is complete, Windows restarts using the settings from the date and time listed above.

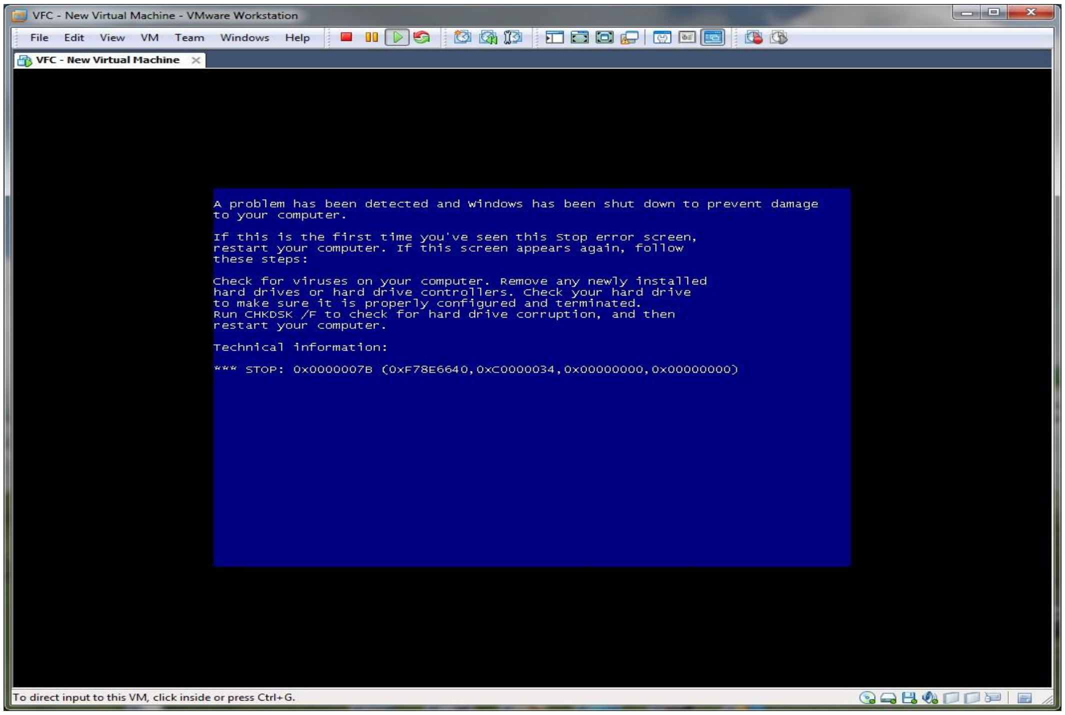
Important: Before continuing, save your changes and close any open programs.

System Restore may take a moment to collect information about the selected restore point before shutting down your computer.

To restore your computer to this date and time, click Next.

< Back | Next > | Cancel

3. Re-start the VM and confirm that it starts normally. It may enter a reboot loop or fail with a message similar to the following:

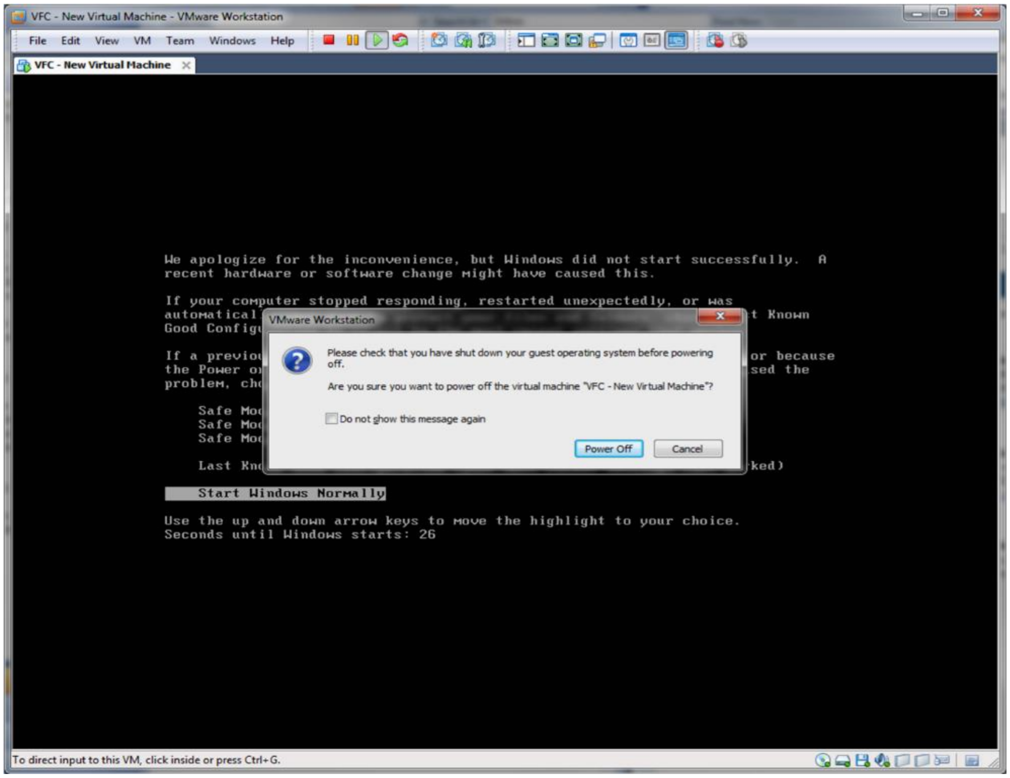


VFC - New Virtual Machine - VMware Workstation
File Edit View VM Team Windows Help
VFC - New Virtual Machine
To direct input to this VM, click inside or press Ctrl+G.

```
A problem has been detected and windows has been shut down to prevent damage
to your computer.

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check for viruses on your computer. Remove any newly installed
hard drives or hard drive controllers. Check your hard drive
to make sure it is properly configured and terminated.
Run CHKDSK /F to check for hard drive corruption, and then
restart your computer.

Technical information:

*** STOP: 0x0000007B (0xF78E6640,0xC0000034,0x00000000,0x00000000)
```

4. This behaviour is very common and occurs because the VMware storage drivers that were injected into the VM by VFC have been removed.

5. To resolve this problem, **Power Off** the virtual machine (do not suspend it):


VFC - New Virtual Machine - VMware Workstation
File
Edit
View
VM
Team
Windows
Help
VFC - New Virtual Machine
To direct input to this VM, click inside or press Ctrl+G.

```
We apologize for the inconvenience, but Windows did not start successfully.  A
recent hardware or software change might have caused this.

If your computer stopped responding, restarted unexpectedly, or was
automatical                                                          t Known
Good Configu

If a previou                                                         or because
the Power o                                                          sed the
problem, ch

    Safe Mod
    Safe Mod
    Safe Mod

    Last Kno                                                         ked)

    Start Windows Normally

Use the up and down arrow keys to move the highlight to your choice.
Seconds until Windows starts: 26
```

VMware Workstation

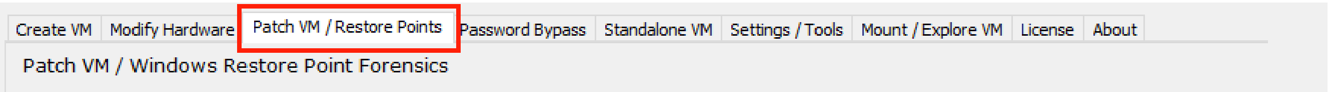
Please check that you have shut down your guest operating system before powering off.

Are you sure you want to power off the virtual machine "VFC - New Virtual Machine"?

□ Do not show this message again

Power Off | Cancel

6. Open the **Patch VM / Restore Points** tab in VFC:

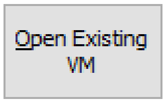


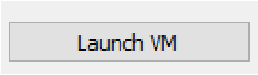
7. Follow the instructions in the earlier section to repair the VM and then launch it again.

8. Restart the VM

Re-Open an existing VM

VFC allows an existing virtual machine to be re-opened and launched in VMware. This can be done using either the **Open Existing VM** button on the **Create VM** tab or via one of the **Launch VM** tabs located elsewhere within VFC:



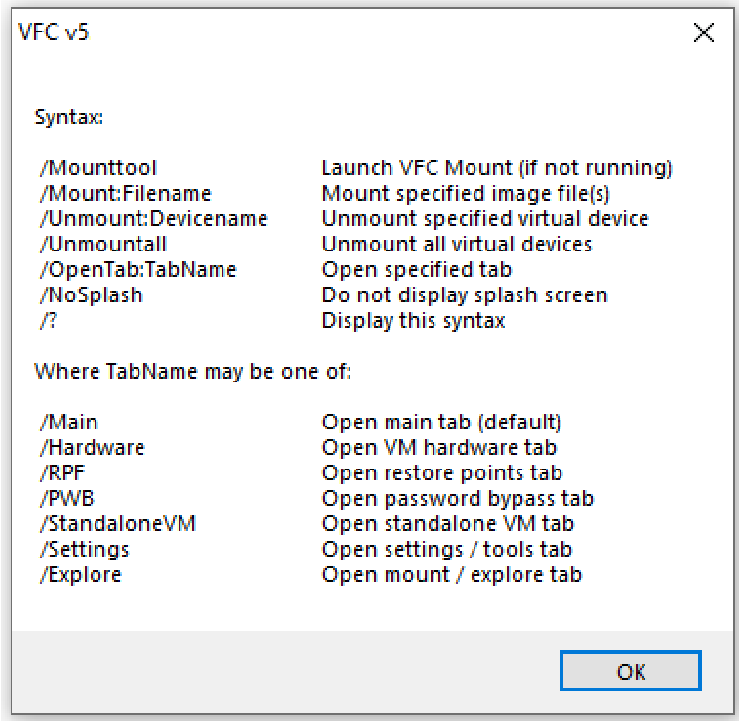


These buttons are provided for convenience and allow you to quickly use the virtual machine after creating or modifying it using VFC. You can also achieve the same outcome by launching the VM directly with VMware.

TIP: Please remember that a VFC created virtual machine relies on one or more emulated physical disks. These are provided by VFC Mount or other third-party mount tools. Please remount any requires images (in the same order) before attempting to launch a VM.

VFC Command Line Interface (CLI)

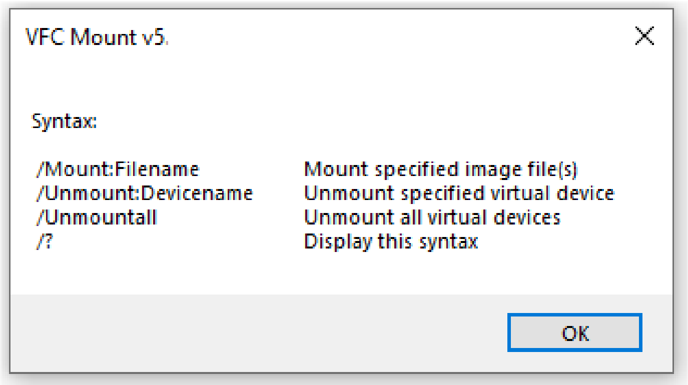
VFC also supports a command-line interface (CLI). This can be used to automate certain VFC tasks and is typically used in batch processes that image and then create virtual machines with little manual intervention. The supported commands can be displayed by using the **VFC5.EXE /?** Command:



```
Syntax:

/Mounttool                  Launch VFC Mount (if not running)
/Mount:Filename             Mount specified image file(s)
/Unmount:Devicename         Unmount specified virtual device
/Unmountall                 Unmount all virtual devices
/OpenTab:TabName            Open specified tab
/NoSplash                   Do not display splash screen
/?                          Display this syntax

Where TabName may be one of:

/Main                       Open main tab (default)
/Hardware                   Open VM hardware tab
/RPF                        Open restore points tab
/PWB                        Open password bypass tab
/StandaloneVM               Open standalone VM tab
/Settings                   Open settings / tools tab
/Explore                    Open mount / explore tab
```

The VFC Integration components for EnCase and X-Ways Forensics use the VFC CLI interface. Please see the section below for further details. The **/MOUNT** and **/UNMOUNT** commands directly interface with the VFC Mount too. This avoids the need to separately launch VFC Mount.

In some cases, it may be useful to directly command VFC Mount via the CLI interface. To view the supported syntax, use the command: **VFCMOUNT32.EXE /?** or **VFCMOUNT64.EXE /?**:



```
Syntax:

/Mount:Filename             Mount specified image file(s)
/Unmount:Devicename         Unmount specified virtual device
/Unmountall                 Unmount all virtual devices
/?                          Display this syntax
```

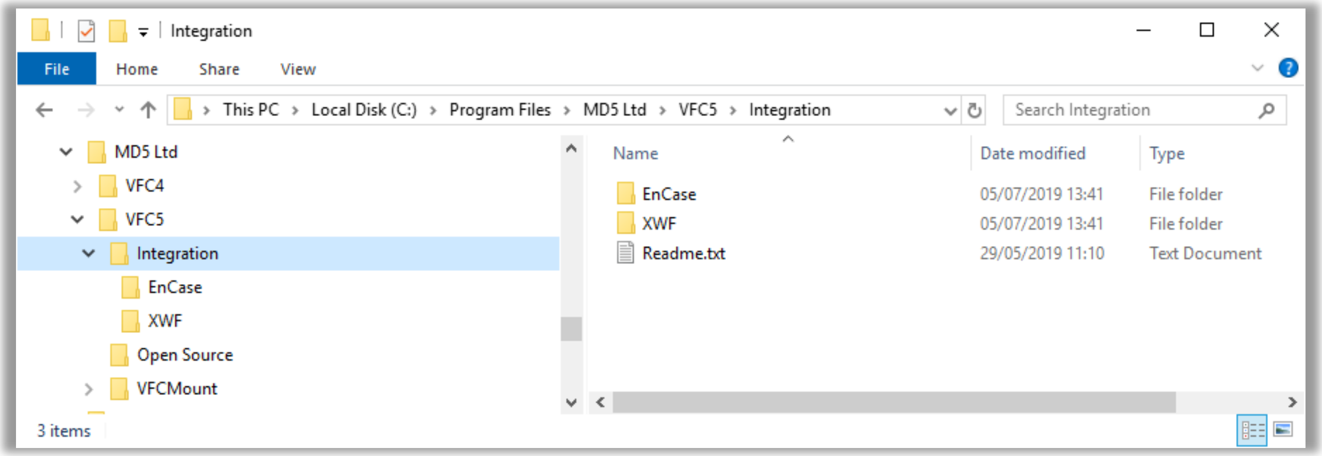
VFC CLI integration with third-party forensic analysis tools

VFC ships with integration components for the following third-party analysis tools:

- X-Ways Forensics X-Tension (v18 and later)
- EnCase EnScript (v6 and later)

The integration components allow you to directly launch VFC from within the above forensic analysis suites and quickly create and launch a virtual machine from the case files.

The integration components are located in the **Integration** sub-folder of the VFC installation:



This PC › Local Disk (C:) › Program Files › MD5 Ltd › VFC5 › Integration

- MD5 Ltd
  - VFC4
  - VFC5
    - Integration
      - EnCase
      - XWF
    - Open Source
    - VFCMount

Name	Date modified	Type
EnCase	05/07/2019 13:41	File folder
XWF	05/07/2019 13:41	File folder
Readme.txt	29/05/2019 11:10	Text Document

Whilst the integration components operating in different ways, they all ultimately provide the same functionality:

- Directly mount supported case image files in VFC Mount (.E01, .Ex01 etc.) *
- Prepare VFC environment for VM creation
- Allow a VM to be created and booted in ~ 2 minutes

* Currently the EnCase EnScript only supports .E01 and.Ex01 format images. This is a limitation of EnCase. The X-Ways Forensics X-Tension supports any formats supported by both by X-Ways and VFC Mount. In some cases (e.g. .AFF4) a third-party plug-in may be required to enable specific image support in X-Ways.

TIP: Before attempting to use the third-party integration components, please start VFC, mount an image using VFC Mount and manually create a VM at least once. This ensures all of the underlying features are enabled.

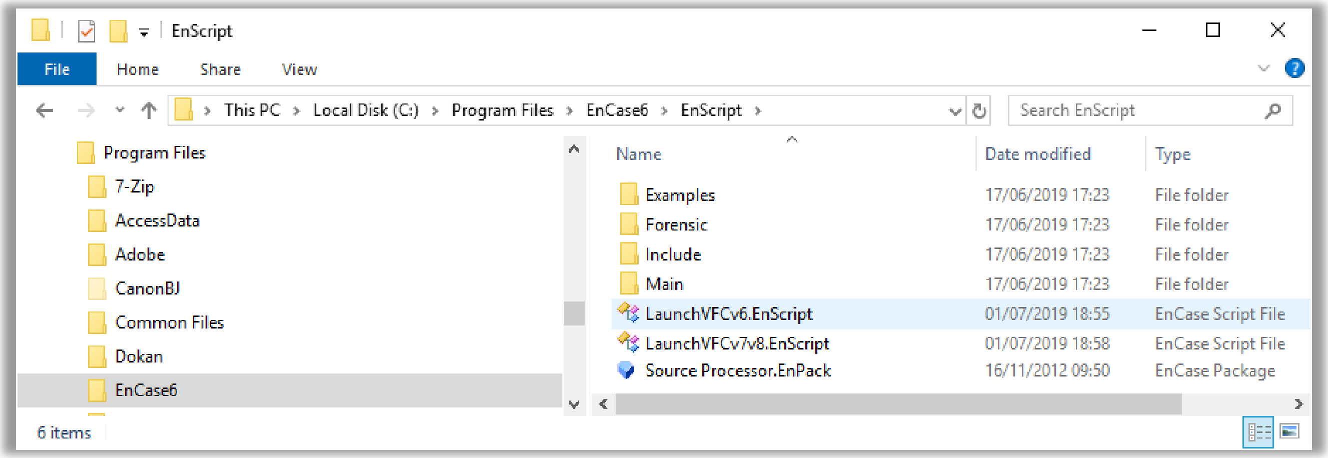
EnCase Integration

Please see your EnCase documentation for detailed instructions on how to install and use EnScripts. The following walkthrough describes the process for EnCase v6 (the instructions for v8 are slightly different). Please proceed as follows:

1. Confirm that VFC/VFC Mount are operational by manually mounting and image and creating a VM at least once.

2. Locate the EnCase **EnScript** folder

3. Copy the appropriate **LaunchVFCvXXX.EnScript** from the VFC **Integration** folder to the **EnScripts** folder:



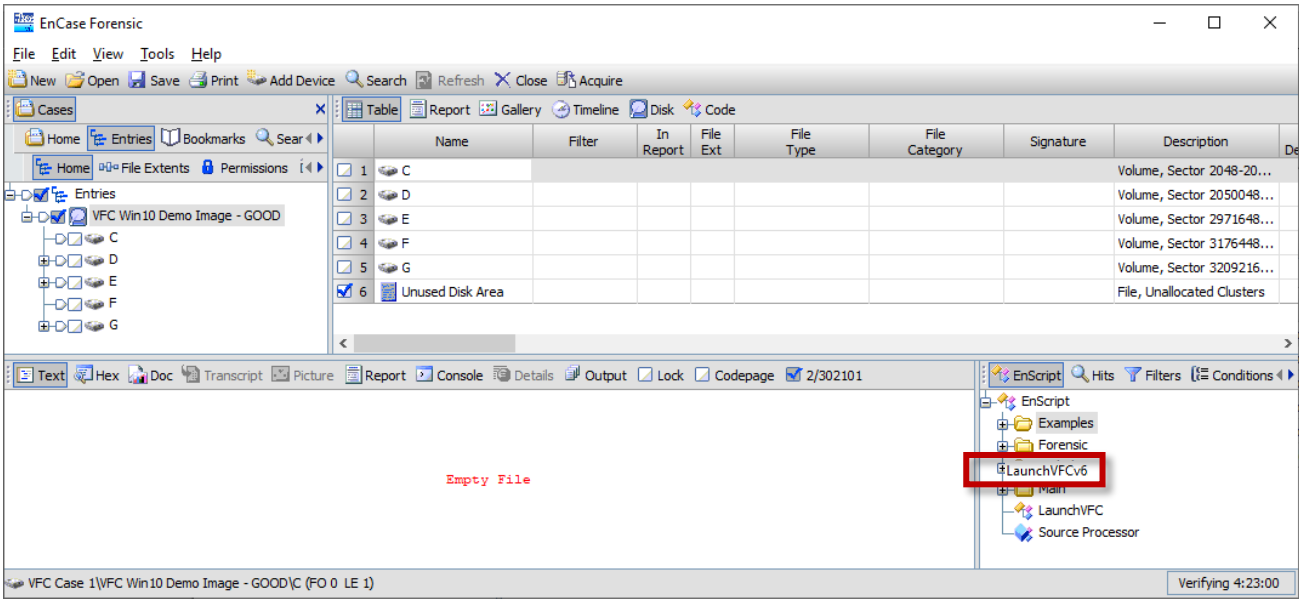
This PC › Local Disk (C:) › Program Files › EnCase6 › EnScript ›

Name	Date modified	Type
Examples	17/06/2019 17:23	File folder
Forensic	17/06/2019 17:23	File folder
Include	17/06/2019 17:23	File folder
Main	17/06/2019 17:23	File folder
LaunchVFCv6.EnScript	01/07/2019 18:55	EnCase Script File
LaunchVFCv7v8.EnScript	01/07/2019 18:58	EnCase Script File
Source Processor.EnPack	16/11/2012 09:50	EnCase Package

6 items

4. Restart EnCase

5. EnCase should discover the new EnScript and display it in the EnScript panel (normally bottom right):


EnCase Forensic
File Edit View Tools Help
New Open Save Print Add Device Search Refresh Close Acquire
Cases
Home Entries Bookmarks Sear
Home File Extents Permissions
Table Report Gallery Timeline Disk Code
Entries
VFC Win10 Demo Image - GOOD
C
D
E
F
G
Text Hex Doc Transcript Picture Report Console Details Output Lock Codepage 2/302101
Empty File
EnScript Hits Filters Conditions
EnScript
Examples
Forensic
LaunchVFCv6
Main
LaunchVFC
Source Processor

	Name	Filter	In Report	File Ext	File Type	File Category	Signature	Description
□ 1	C							Volume, Sector 2048-20…
□ 2	D							Volume, Sector 2050048…
□ 3	E							Volume, Sector 2971648…
□ 4	F							Volume, Sector 3176448…
□ 5	G							Volume, Sector 3209216…
☑ 6	Unused Disk Area							File, Unallocated Clusters

VFC Case 1\VFC Win10 Demo Image - GOOD\C (FO 0 LE 1)

Verifying 4:23:00

6. Create a new EnCase case (or load a previous case) containing the relevant disk image(s)

7. Execute the **LaunchVFCvXXX.EnScript**. This will:

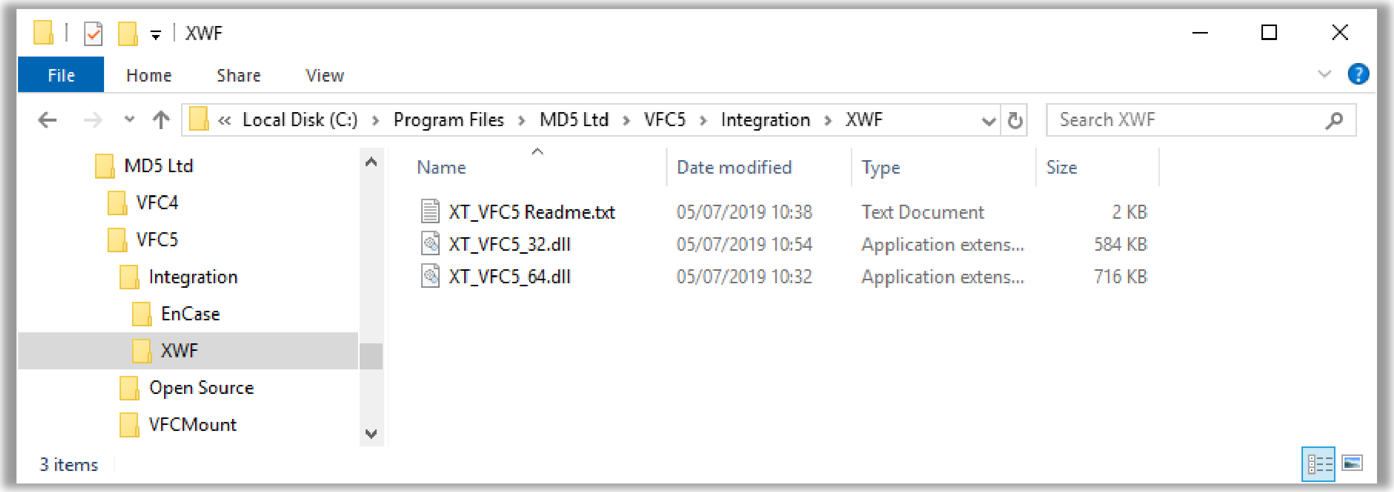
    - Mount each supported image in VFC Mount
    - Launch VFC and prepare to create the VM

8. Follow the normal VFC process to select any remaining VM options and create the VM

X-Ways Forensics Integration (XWF)

Please see your X-Ways (XWF) documentation for detailed instructions on how to install and use third-party X-Tension DLLs. The following walkthrough describes the process for X-Ways v18. Please proceed as follows:

1. Locate the EnCase **VFC5\Integration\XWF** folder



Name	Date modified	Type	Size
XT_VFC5 Readme.txt	05/07/2019 10:38	Text Document	2 KB
XT_VFC5_32.dll	05/07/2019 10:54	Application extens...	584 KB
XT_VFC5_64.dll	05/07/2019 10:32	Application extens...	716 KB

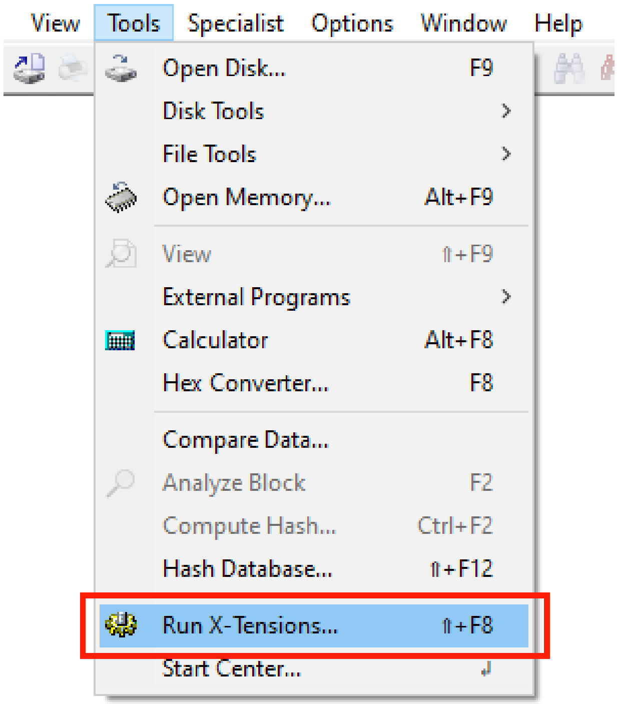
TIP: It may be helpful to copy this folder path to the clipboard.

2. Note the DLL appropriate for your XWF environment. This will be one of:

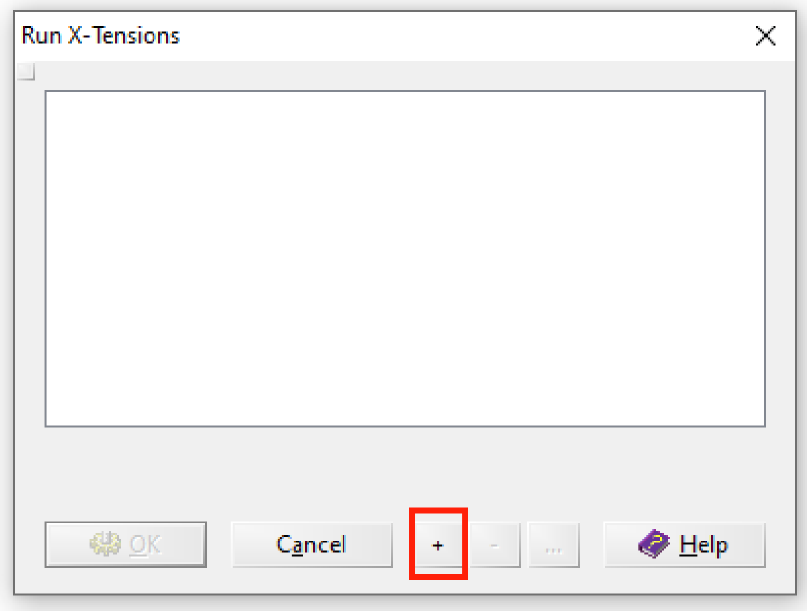
    - For 32-bit XWF use: XT_VFC5_32.DLL
    - For 64-bit XWF use: XT_VFC5_64.DLL

3. Open XWF (v18 or later)

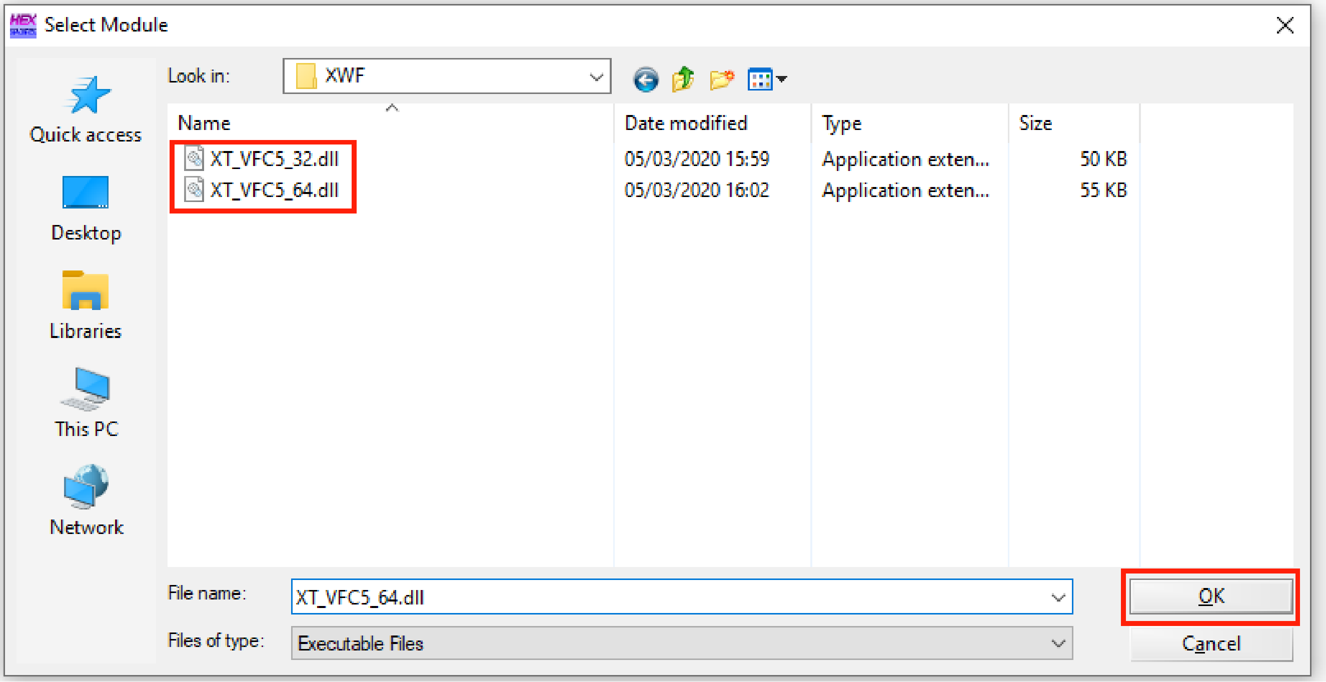
4. Navigate to the **Tools/Run X-Tensions** menu



5. Click + and browse to the folder containing the XT_VFC5_xx.DLL files:



6. Select the appropriate DLL and click **OK:**



Look in: XWF

Name	Date modified	Type	Size
XT_VFC5_32.dll	05/03/2020 15:59	Application exten...	50 KB
XT_VFC5_64.dll	05/03/2020 16:02	Application exten...	55 KB

File name: XT_VFC5_64.dll

Files of type: Executable Files

OK

TIP: There is no need to copy the DLL file to the X-Ways folder. Just point XWF at the "Integration" folder. This will ensure you get the latest X-Tension the next time you upgrade VFC.

To use the X-Tension in XWF proceed as follows:

1. Confirm that VFC/VFC Mount are operational by manually mounting and image and creating a VM at least once.

2. Create a new XWF (or load a previous case) containing the relevant disk image(s)

3. Navigate to the **Tools / Run X-Tensions** menu

4. Double click the **XT_VFC5_xx.DLL** file and follow the on-screen prompts. This will:

   - Mount each supported image in VFC Mount
   - Launch VFC and prepare to create the VM

5. Follow the normal VFC process to select any remaining VM options and create the VM